LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

CASE: YRITYS - X

TIETOTURVAKARTOITUS

LAHDEN
AMMATTIKORKEAKOULU
Liiketaloudenlaitos
Tietojenkäsittelyn koulutusohjelma
Suuntautumisvaihtoehto
Opinnäytetyö
Syksy 2012
Atte Arkko

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

ARKKO, ATTE: Case:Yritys-X Tietoturvakartoitus

Tietojenkäsittelyn opinnäytetyö, 44 sivua, 2 liitesivua

Syksy 2012

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee tietoturvakartoituksen tuottamista. Tarkoituksena oli selvittää kohdeyrityksen tietoturvan nykytaso, sekä antaa kohdeyritykselle tietoa, miten se voisi parantaa tietoturvaansa ja millaisilla työkaluilla tietoturvan tasoa voidaan mitata.

Teoriaosuudessa käsitellään tietoturvaa yleisesti, sekä tarkastellaan, mitä hallinnollisen tietoturvan tulisi sisältää. Teoriaosassa käydään läpi myös suojattavat kohteet, sekä tiedon luokittelu. Teoriassa esiintyvät taulukot perustuvat laadukkaisiin ja tunnettuihin tietoturvan ISO-standardeihin.

Empiirisessä osuudessa pureudutaan kohdeyrityksen tietoturvan nykytilaan ja tarkastellaan sitä teorian pohjalta. Empiriassa kartoitetaan mm. yrityksen suojattavat kohteet, henkilöstön tietoturvan tietämyksen tasoa, sekä määritellään kohdeyrityksen merkittävimpiä uhkia ja arvioidaan niiden aiheuttamaa haittaa, sekä toteutumisen todennäköisyyttä.

Loppu päätelmissä todetaan, että yrityksen tietoturva on hyvällä tasolla. Yritys voisi kuitenkin haluttessaan parantaa tietoturvaansa entisestään pienilläkin muutoksilla. Loppu päätelmissä todettiin myös, että henkilöstöllä oli hyvä tietoturvan perustietämys. Päätelmissä tuotiin esille myös yritykselle annetut työkalut, joilla se voi helposti tarkastella tietoturvansa tilaa. Seuraava askel yrityksellä olisi tuottaa tietoturvasuunnitelma.

Viimeisessä luvussa, tietoturvan tulevaisuus pohditaan, miltä tietoturvan tulevaisuus yleisesti yrityksissä näyttää.

Avainsanat: tietoturva, tietoturva-analyysi, hallinnollinen tietoturva, tietoturvakartoitus, tietoturva selvitys

Lahti University of Applied Sciences
Degree Programme in …

ARKKO, ATTE: Case: Company-X Information security inspection

Bachelor's Thesis in Business Information Systems 44 pages, 2 appendices

Autumn 2012

ABSTRACT

This thesis deals with information security inspection to company X (name hidden). The purpose of the study was define current level of information security in company X. Secondary purpose was give information, how company could make their information security better and tools for measuring it levels.

The theoretical part determines what is information security. Also look a bit closer administrative security and what it should contain. Theory part also delves what should be protected and how to categorize information.

The empiricism part sinks into the company X current condition of information security. It determines targets that contains important information and requires protection. Also determine the highest threats and evaluate the cons caused by them and also the probability that it come true.

In summary we can say that company X has decent information security level. Company X could easily increase its information security level with small effort. We can also summarize that employees have good basic level concerning information security. Next step for company is to create information seciurity plan.

Last we look what will be future of information security and how it going to look and effect in companies.

Key words: information security, administrative security, information security inspection, information security plan.

SISÄLLYS

1 JOHDANTO

Tietoturvasta huolehtiminen on nykyään yksi tärkeimmistä asioista yritysten arkea. Lainsäädännön vaatimukset ja asiakkaiden jatkuvasti muuttuvat tietoturvatarpeet ovat yksi merkittävä syy, miksi yritykset parantavat toimintatapojaan. Yritys X (nimi salattu) on todennut, että yrityksen kasvaessa yhden miehen yrityksestä usean työntekijän yritykseksi, olisi hyvä aika tehdä kartoitus tietoturvan nykytilasta yrityksessä. Yritys X antoi minulle toimeksiannon toteuttaa yritykseen tietoturvakartoitus, jonka pohjalta yrityksen on helpompi tehdä tietoturvasuunnitelma. Aiheeltaan tutkimus ei ole uusi, se on silti hyvin ajankohtainen yritysten päivittäisessä arjessa. Tietoturvasta on tuotettu paljon materiaalia suuntautuen isoihin organisaatioihin, joten tietoa on sovellettava toimivaksi kokonaisuudeksi pienemmille yrityksille. Tietolähteinä toimivat internet sekä kirjallisuus. Aluksi käydään läpi päättötyön tavoitteet, sekä tutkimus ongelmat. Seuraavaksi tarkastellaan, mitä on tietoturva, sekä mitä tietoturvakartoituksessa tulisi ottaa huomioon. Lopuksi tehdään Yritys X:lle tietoturvakartoitus sekä tuodaan esille kehitysehdotuksia. Lähteinä käytetään suomalaisia ja ulkomaalaisia kirjoja, virallisia tietoturvastandardeja sekä sähköistä materiaalia.

1.1 Tutkimuksen tavoitteet ja tutkimusongelmat

Kohdeyrityksen tavoite on parantaa omaa tietoturvatasoaan. Yritys X kokee, että henkilöstömäärän kasvaessa muutamasta henkilöstä lähes 10 hengen yritykseksi on hyvä tarkastaa tietoturvan nykytila. Tämän päättötyön tarkoituksena on, antaa Yrityksen X johdolle kuva siitä, mikä on Yritys X:n todellinen tietoturvan tila tällä hetkellä, sekä tuoda esille kehitysehdotuksia.

Tämän opinnäytetyön päätutkimusongelmana on

- Mikä on Yritys X:n tietoturvan nykytila?

Alaongelmat ovat

- Miten Yritys X voisi parantaa tietoturvaansa?
- Tarvitseeko henkilöstö tietoturvakoulutusta?

1.2 Tutkimusmenetelmät ja aiheen rajaus

Opinnäytetyö toteutettiin case-tutkimuksena, toiselta nimeltään tapaustutkimuksena. Tapaustutkimuksessa on tarkoitus kerätä yksityiskohtaista, sekä intensiivistä tietoa yksittäisestä kohteesta. Tapaustutkimuksessa aineistoa kerätään useilla metodeilla, kuten mm. havainnoinnilla, haastatteluilla, sekä dokumentteja tutkimalla. Tavoitteena on tyypillisimmin ilmiöiden kuvailu. (Hirsjärvi, Remes & Sajavaara 2009, 130-131.)

Tutkimus on luonteeltaan Kvalitatiivinen, eli laadullinen tutkimus. Tutkimustapa määräytyi kvalitatiiviseksi, koska tutkimuksessa tarkastellaan juuri kohdeyrityksen tietoturvan nykytilaa ja sen laatua. (Taloustutkimuslaitoksen verkkosivu 2012)

Tutkimus on luonteeltaan deduktiivinen, sillä tutkimus ei luo uutta teoriaa, vaan tarkastelee kohdeyrityksen tietoturvan nykytilaa jo olemassa olevan teorian pohjalta. (Virtuaali AMK verkkosivu 2012)

Tutkimusmenetelminä on käytetty havainnointia, kyselytutkimusta sekä teemahaastattelua. Havainnointi on tapahtunut tutkijan osalta niin, että hän on ollut työharjottelussa yrityksen alaisuudessa ja havainnoinut yrityksen toimintatapoja tietoturvan osalta. Tutkijalla on siis aktiivinen rooli havainnoitavassa toiminnassa eli havainnointi on osallistuvaa havainnointia. (Routio 2007, 1.)

Tutkimuksen haastattelut toteutettiin teemahaastatteluna. Teemahaastattelu on lomakehaastattelun ja avoimen haastattelun välimuoto. Teemahaastattelu etenee ennakolta mietittyjen teemojen varassa, mutta haastattelutilanteissa on liikkumavaraa. Avoimilla kysymyksillä voidaan saada esille asioita, joita haastattelija ei

ole suoranaisesti osannut kysyä. (Tilastokeskuksen verkkosivu 2012) Teemahaastattelu toteutettiin yrityksen johdolle. Aihe rajattiin yrityksen tietoturvauhkien kartoitukseen, sekä uhkan toteutumisen ja haitan määrän arvioimiseen. Teemahaastattelussa ei käytetty valmista aineistoa, vaan se luotiin haastattelun aikana. Ainoastaan haastattelun teemat eli tietoturvan osa-alueet oli eritelty ennen haastattelua.

Kyselytutkimus suoritettiin työntekijöille. Tavoitteena kyselyssä oli selvittää työntekijöiden tietoturvatietämystä sekä kiinnostusta tietoturvaan. Kysely tehtiin kirjallisena kyselynä yhden päivän aikana. Henkilöt vastasivat avoimiin kysymyksiin. Vastaajille ei siis annettu vastausvaihtoehtoja, vaan he joutuivat vastaamaan itsenäisesti. (Routio, 2007, 2)

Tutkimus rajoittuu ainoastaan tietoturva-analyysiin yrityksen nykytilasta sekä kehitysehdotuksiin. Tarkoituksena ei ole tuottaa tietoturvasuunnitelmaa, johtuen aiheen laajuudesta. Ainoastaan analysoida nykytilaa tietoturvan osa-alueiden kautta (fyysinen tietoturva, henkilöstöturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoliikenneturvallisuus). Myös tietoliikenneturvallisuutta osa-alueena rajattiin. Tietoliikenneturvallisuudessa tarkastellaan ainoastaan yrityksen käyttämiä ulkoisia palveluita, sekä yleisellä tasolla yrityksen sisäisiä- ja langattomia verkkoja. Suurimmaksi osaksi tutkimuksessa keskitytään kohdeyrityksen tietoturvan eri osa-alueissa ilmeneviin uhkiin, sekä miten yritys on toiminut niiden estämiseksi ja onko keinoja parantaa tietoturvaa entisestään.

Tutkimuksesta on rajattu pois myös nykytila-analyysiin liittyvä kustannusanalyysi, jossa selvitettäisiin eri tietoturvaparannusten kustannuksia. Tämä tulee tietoturvakehittämisprojektin myöhemmässä vaiheessa, yrityksen aloittaessa tietoturvan uudistusprojektin.

1.3 Opinnäytetyön rakenne

KUVIO 1. Työn rakenne

Opinnäytetyö koostuu kuudesta eri luvusta (Kuvio 1). Luvut muodostuvat teoriaosuudesta, sekä empiirisestä osasta. Ensimmäinen luku eli johdanto esittelee tutkimuksen aihetta, tavoitteita ja tutkimus ongelmaa. Lisäksi käydään läpi työn rakenne.

Toinen, kolmas ja neljäs luku koostuu tutkimuksen teoriasta. Toisessa luvussa käydään läpi yleisesti mitä tietoturva on. Kolmannessa luvussa määritellään mitä hallinnollinen tietoturva sisältää, sekä esitellään työkalu tietoturvariskien määrittelemiseen. Neljännessä luvussa määritellään, mitä olisi hyvä ottaa huomioon tietoturva kartoitusta suunniteltaessa.

Viides luku käsittelee tietoturvakartoitusta kohdeyritykselle, sekä yritykseen kohdistuvia tietoturva uhkia tarkasteltuna osa-alueiden kautta. Sekä annetaan myös mahdollisia kehitysehdotuksia liittyen eri uhkiin, koskien yrityksen tietoturvaa. Se myös sisältää henkilöstön tietoturvan osaamista mittaavan kyselyn tulokset.

Viimeisessä kuudennessa luvussa käydään läpi mm. opinnäytetyön haasteista, omaa näkemystä, miten päättötyö onnistui sekä mitä opin tehdessäni päättötyötä. Luvussa kerrotaan myös jatkotoimenpide-ehdotuksia yrityksen tietoturvan kehittämiseksi. Lopuksi pohditaan tietoturvan tulevaisuutta yrityksissä.

2 MITÄ ON TIETOTURVA?

Kaikki yritykset omistavat tärkeitä tietoja, jotka he pyrkivät suojaamaan. Tietoturvaksi kutsutaan toimenpiteitä ja tapoja, joilla yritys suojaa tietonsa. (Hakala. ym, 2006, 4.) Syitä suojata tietoja on useita, kuten liikesalaisuuksien suojaaminen, sekä lain asettamat vaatimukset, esimerkiksi henkilötietojen käsittelyssä. Jos yrityksen tietoturva pettää voi se aiheuttaa yritykselle rahallista menetystä, ongelmien korjaaminen voi tuoda lisää kustannuksia. Yritys voi joutua myös oikeudelliseen vastuuseen, ja näin kustannukset voivat nousta ennestään. Pahimmassa tapauksessa yrityksen imago voi kärsiä ison kolauksen heikon tietoturvan vuoksi. (ESS verkkosivu, 22.10.2012) Voidaan siis sanoa, että rahallinen panostaminen tietoturvaan kannattaa, sillä puutteet tietoturvassa voivat aiheuttaa enemmän kustannuksia, kuin hyvän tietoturvan ylläpitäminen.

On kuitenkin hyvä muistaa, että ei ole olemassa täydellistä tietoturvaa, joka takaisi kokonaisvaltaisen turvan kaikilta uhkilta. Tietoturvan tarkoitus on hallita uhkia, ei poistaa niitä lopullisesti. Tietoturva auttaa varautumaan ennalta kartoitettuihin riskeihin ja siten nopeuttaa onnettomuuksista toipumista.

2.1 Tietoturvallisuuden ulottuvuudet

Tietoturvallisuutta voidaan tarkastella kolmen ulottuvuuden kautta, luottamuksellisuus, eheys ja saatavuus. Tämä on perinteinen tapa määritellä tietoturvan ulottuvuuksia. Sitä kuitenkin voidaan pitää hyvin pelkistettynä. Siksi tietoturvallisuuden voidaan katsoa sisältävän vielä kolme muuta ulottuvuutta, todentaminen, tunnistaminen ja kiistämättömyys (Mietinen, 1999, 23-28.)

Luottamuksellisuudella tarkoitetaan, että tieto on saatavissa ainoastaan henkilöille, järjestelmille tai prosesseille, joilla on oikeus käyttää kyseistä tietoa. Eikä tietoa paljasteta tai muutoin anneta sivullisten tietoon. (Viestintäviraston verkkosivu 2012; ISO/IEC 17799 2000, 1; ISO/IEC 27001 2005, 2.)

Eheydellä tarkoitetaan, että tiedot, järjestelmät, palvelut ja laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena eivät ole muuttuneet, vahingoittuneet tai tuhoutuneet. Esimerkiksi tietojärjestelmän virhe tai haittaohjelma voisi aiheuttaa muutoksia tiedoissa, jolloin tieto olisi virheellistä, eikä eheyttä voitaisi enää taata. Tiedon eheyttä voidaan pyrkiä varmistamaan tekemällä säännölliset varmuuskopiot. Tiedon muuttuminen on voitava huomata, sekä jäljittää, jotta varmuuskopioinnista olisi hyötyä. (Viestintäviraston verkkosivu 2012; ISO/IEC 17799 2000, 1; ISO/IEC 27001 2005, 2.)

Saatavuudella ja käytettävyydellä tarkoitetaan, että tiedot, järjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen saatavilla ja esteettä hyödynnettävissä. Jotta hyvä saatavuus voidaan varmistaa, pitää järjestelmiä ja fyysisiä laitteita huoltaa säännöllisesti ja tarpeen mukaan. Näin voidaan varmistaa, että tieto on aina saatavilla. Tietojen tuhoutuessa toimivista ja ajantasaisista varmuuskopioista voidaan palauttaa tietojen saatavuus. (Viestintäviraston verkkosivu 2012; ISO/IEC 17799 2000, 1; ISO/IEC 27001 2005, 2)

Todentamisella pyritään tunnistamaan luotettavasti henkilön identiteetti. Esimerkiksi tunnuksella ja salasanalla, pyritään todentamaan, että henkilö, joka palvelimelle kirjautuu on juuri se kuka ilmoittaa olevansa. Todentamista siis tarpeellinen, jotta voidaan taata luottamuksellisuus ja eheys. (Viestintäviraston verkkosivu; Raggad 2009.)

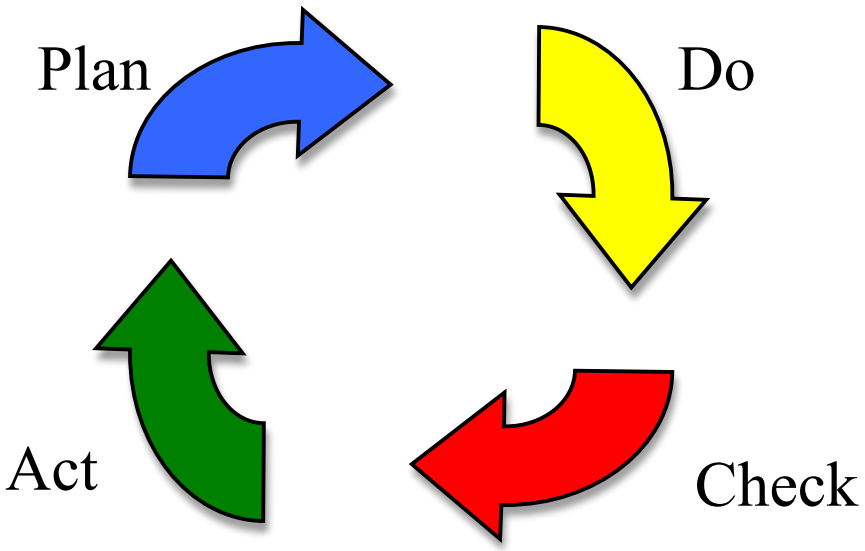
Tunnistamisella tarkoitetaan menettelytapaa, jolla yksilöidään kohde, kuten käyttäjä tai järjestelmä. Tunnistus ei kuitenkaan välttämättä vaadi kohteelta toimenpiteitä. Tunnistamisella tarkoitetaan esimerkiksi työtovereiden tunnistamista työyhteisöön kuuluviksi.(Viestintäviraston verkkosivu 2012)

Kiistämättömyys pyrkii luomaan todisteita, että todennettu ja tunnistettu henkilö ei voi kiistää suorittamiaan toimia järjestelmässä. Kaikki henkilön tekemät toimet ja muutokset tallentuvat järjestelmään. (Viestintäviraston verkkosivu 2012; Caelli & McCullagh 2000.)

3 MISTÄ HALLINNOLLINEN TIETOTURVA KOOSTUU?

Hallinnollinen tietoturva sisältää menettelytavat muiden tietoturva osa-alueiden ohjaamiseen. Tavoite on varmistaa, että jokainen osa-alue on riittävällä tasolla, sekä pyrkiä pitämään huolta, ettei yrityksen toiminta ole lainvastaista. Hyvän tietoturvan toteuttamisen osalta on tärkeää, että yrityksen hallinto on sitoutunut ylläpitämään, päivittämään ja noudattamaan asetettua tietoturvapolitiikkaa. Hallinnon on myös ymmärrettävä tietoturvan tärkeys yrityksen kannalta.

Hallinnollisen tietoturvan tärkeimpiä tehtäviä on huolehtia, että henkilöstön tietoturvaosaaminen olisi vähintäänkin riittävällä tasolla. Esimerkiksi henkilöstö, joka ymmärtää tietoturvasta tuottaa pienemmän riskin kuin henkilöstö, joka ei ymmärrä tietoturvasta mitään. (Maiwald 2002, 118.) On myös mahdollista, että henkilökuntaa neuvomalla saadaan tehokkaita tuloksia yrityksen tietoturvaan hyvinkin pienillä kustannuksilla. Tärkeintä on, että henkilöstö tiedostaa olemassa olevat riskit. (Ruohonen 2002, 5; Hakala ym.2006, 10-11)



Kuva1. PDCA-malli (ISO/IEC 20071:fi 2006, 8).

Tietoturvan hallintajärjestelmän kehittämiseen suositellaan PDCA-mallia (Plan-Do-Check-Act). Suomen kielinen vastine on, suunnittele – toteuta – arvioi – Toimi. Kuvan1. PDCA-mallia sovelletaan seuraavasti: Suunnitteluvaiheessa määritellään kohteet, joita halutaan suojata, määritellään millainen tietoturvantaso yritykselle halutaan ja lopuksi tuotetaan tietoturvan hallintajärjestelmä. Kun tilanne muuttuu, suunnittelu ja muut toimenpiteet aloitetaan alusta. Näin prosessi on jatkuvasti toiminnassa, joka mahdollistaa sen kehittymisen. (Hakala ym. 2006, 106.)

3.1 Tietoturvapolitiikka

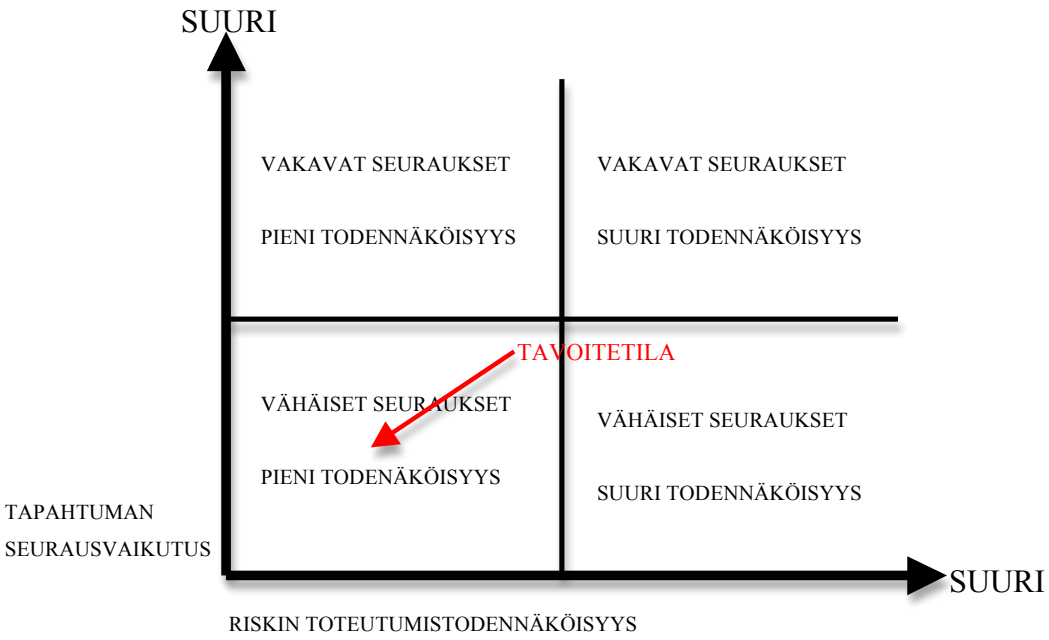
Tietoturvapolitiikka on yksinkertaisesti yrityksen johdon linjaamat toimintatavat tietoturvan edistämiseksi. Tietoturvapolitiikan tehtävä ei ole suoranaisesti kertoa yksityiskohtaisia ohjeita, mitä tehdään ja miten tehdään, vaan se on enemmänkin suuntaa-antava. Siinä määritellään yrityksen strategiset tavoitteet tietoturvan osalta. (Baskerville ym. 2008, 124-126.) Dokumentti tulisi kirjoittaa selkeällä kielellä ja sen ymmärtämisen ei tulisi vaatia erityisosaamista. Kun yrityksen tarpeet ja tilanteet muuttuvat tulisi tietoturvapolitiikka päivittää ajantasalle (Laaksonen ym. 2006, 146).

3.1.1 Toipumissuunnitelma ja riskienhallinta

Toipumissuunnitelma käsittelee tietoturvaonnettomuuksista selviämistä. Dokumentin tulisi sisältää kirjalliset ohjeet niistä toimenpiteistä, joilla yritys selviytyy erilaisissa poikkeustilanteissa (Laaksonen ym. 2006, 227). Toipumissuunnitelmaa luodessa tulisi selvittää, mitkä toiminnot ovat yritykselle tärkeimpiä. Niitä ovat esimerkiksi palkanmaksu, asiakkaiden palvelu, logistiikka ja tuotteiden myynti. Kun tärkeimmät toiminnot on listattu, tulisi arvioida, kuinka kauan eritoiminnot voivat olla pois toiminnasta ja miten nopeasti ne saadaan palautettua takaisin normaalitoimintaan, ennen kuin yritys kärsii liiallista vahinkoa. (Raggad 2010, 217-218.) On myös huomioitava, miten paljon tiedoista voi hävitä, ennen kuin yritys kärsii merkittävistä ongelmista (Geogory 2008, 18-20).

Toipumissuunnitelman tulisi sisältää riskianalyysi. Riskianalyysissä määritellään yrityksen tärkeisiin tietoihin tai toimintoihin vaikuttavia uhkia. Uhkien seurausvaikutusten arvioinnilla pystytään hahmottamaan, millä tavalla uhkatekijä voi vaikuttaa yrityksen päivittäiseen toimintaan. Riskiä voidaan luonnehtia kolmen peruselementin uhkan, epävarmuuden ja mahdollisuuden kautta. Usein yritykset keskittyvät riskeihin, jotka aiheuttavat yrityksen toiminnalle vahinkoa. Riskiä tarkastelemalla pyritään tunnistamaan sen aiheuttamat uhkat, jotta niitä vastaan voidaan suojautua. Epävarmuus on aina olemassa, koska yritys ei voi koskaan olla varma riskin toteutumisesta tai toteutumattomuudesta ja siksi olisi hyvä selvittää riskin vaihteluväli sen todennäköisyyden arvioimiseksi. (VTT 2009)

Riskianalyysin toteuttamiseen voidaan käyttää kuvion2 mallia. Kuvan nelikenttää käytetään yleisesti riskien hallinnan havainnollistamisessa ja sitä sovelletaan tässä yhteydessä tietoturvallisuus riskien kuvaamiseen.



Kuvio2 Tietoturvallisuusriskien tavoitetila

Tietoturvallisuusriskien tavoitetila asettuu kuvio 2 alakulmaan. Tämän ryhmänriskit ovat seurauksiltaan vähäisiä, ja niiden toteutuminen on epätodennäköistä. Kaikkien muiden neljänneksien tietoturvallisuusriskit on pyrittävä saamaa tilaan, jossa ne lähestyvät kokoajan kuvan vasenta alakulmaa. Näiden riskien toteutumisella ei ole merkittävää vaikutusta yrityksen liiketoimintaan ja niiden toteutuminen on epätodennäköistä. (Miettinen 1999, 58.)

3.2 Riskin käsittely

Riskin poistaminen

Yritys voi pyrkiä poistamaan riskin, joka uhkaa yrityksen tietoturvaa. Näin riski katoaa ja ei enää ole uhka yrityksen tietoturvalle. Riskin poistaminen on kuitenkin lähes mahdotonta, sekä runsaasti resursseja ja kustannuksia vaativa prosessi. Tästä syystä tietoturvallisuusriskejä harvoin pyritään poistamaan kokonaan. (Miettinen 1999, 56)

Riskin pienentäminen

Selkeästi yleisin tapa hallita yritykseen kohdistuvia tietoturvallisuus riskejä, on pyrkiä pienentämään niiden mahdollisia seurausvaikutuksia. Useimmat nykyisin käytettävät suojausmenetelmät ovat luonteeltaan sellaisia, että niillä ei voida poistaa riskejä kokonaan, mutta niitä käyttämällä voidaan pienentää tietoturvallisuuteen kohdistuvia riskejä merkittävästi. (Miettinen 1999, 56-57)

Riskin siirto

Yritys voi myös siirtää omaa tietoturvaa uhkaavan riskin sopimuksen mukaan toiselle osapuolelle. Tyypillisesti tämä toinen osapuoli, kenelle riski siirretään on vakuutusyhtiö. Useat riskit voidaan siirtää toiselle osapuolelle, mutta ei kuitenkaan kaikkia. (Miettinen 1999, 57)

Riskin hyväksyminen

Joskus yritys voi päätyä hyväksymään riskin. Tämä tarkoittaa, että yritys ei tee mitään riskin estämiseksi, vaan riski otetaan tietoisesti. Tähän voidaan päätyä esimerkiksi silloin, kun riskin seuraukset ovat vähäiset ja todennäköisyys riskin toteutumiselle on todella pieni (tavoitetila) tai yksinkertaisesti kyseiselle riskille ei voida tehdä mitään. (Miettinen 1999, 57)

4 MITÄ OTTAA HUOMIOON TIETOTURVA KARTOITUKSESSA?

Ensimmäinen askel hyvän tietoturvan rakentamiseen yritykselle on tehdä tietoturvakartoitus. Jotta tietoturvakartoituksesta tulee hyvä ja kattava on se tehtävä yhteistyössä tietoturva asiantuntijoiden, tutkittavan alueen tai kohteen tuntijoiden ja yrityksen päättäjien kanssa. Tietoturvakartoituksessa tulisi keskittyä yhteen kohteeseen kerrallaan, sekä käyttää monia eri menetelmiä uhkien selvittämiseksi. Uhkia määriteltäessä on hyvä muistaa, että kaikkein epätodennäköisimpiin uhkiin ei kannata käyttää aikaa, sillä se olisi ajan ja resurssien haaskausta. (VTT 2009.)

Taulukosta 1 nähdään tietoturvakartoitukseen kuuluvat vaiheet, joihin palaamme tuonnempana. Ensin on kuitenkin ymmärrettävä, mitä tieto ja tietoturva tarkoittavat. Tämän jälkeen voidaan alkaa suunnittelemaan tietoturvakartoitusta. Yritykselle tulisi myös määritellä tavoitetaso, johon tietoturvan osalta vähintäänkin pyritään. Näin yrityksellä olisi vertailukohta, johon verrata tietoturvan nykytilaa. (ISO/IEC 17799 2000.)

Taulukko1. Tietoturvakartoitus vaiheittain (ISO/IEC 17799 2000, Tietoturvaopas 2010).

Vaihe	Kuvaus
Määrittele suojattavat kohteet	Toiminnalle tärkeät tiedot, laitteet yms.
Selvitä suojattavat kohteet	Missä kohteet sijaitsevat, kuka niitä käyttää
Luokittele suojattavat kohteet	Kohteiden tärkeys yrityksen toiminnalle
Määrittele riskit	Kohteisiin liittyvät riskit
Analysoi riskit	Riskien toteutumisen toden näköisyys, haitan suuruus
Määrittele puutteet	Mitkä riskit ovat liian vakavia verrattuna tavoite tasoon

Etsiessäni tietoa tietoturvallisuudesta, huomasin, että suurin osa tiedosta oli selkeästi suunnattu isoille yrityksille, joilla oli resursseja, rahaa ja aikaa käytettäväksi isoihin tietoturva projekteihin. Oli heti selvää, että yritys X, mihin tietoturvakartoitus on tarkoitus luoda, ei ollut niin suuri, että se olisi voinut käyttää näin mittavasti rahaa ja resursseja ostamalla palvelun toiselta yritykseltä. Yrityksellä oli alustava suunnitelma tietoturvasta. Sitä ei kuitenkaan koskaan dokumentoitu. Ollessani yrityksen palveluksessa huomasin yrityksen nykyisessä tietoturvassa puut-

teita. Otin asian rohkeasti esille yrityksen johdon kanssa ja sovimme, että teen aiheesta opinnäytetyön.

4.1 Suojattavat kohteet

Tehtäessä tietoturvakartoitusta on hyvä aloittaa suojattavista kohteista, joihin kuuluvat kaikki yrityksen toiminnalle tärkeät tiedot ja asiat tai niitä sisältävät kohteet. Suojausta tarvitsevat kohteet voidaan jakaa henkilöihin, laitteisiin, tiloihin, palveluihin, aineistoihin ja tietojärjestelmiin. Henkilöihin voidaan määritellä kaikki ne, joita yritys tarvitsee ylläpitääkseen päivittäistä toimintaa. Näitä henkilöitä kutsutaan avainhenkilöiksi. Laitteisiin voidaan määritellä esimerkiksi palvelinympäristöt ja henkilökohtaiset laitteet: puhelimet, tabletit ja kannettavat. Yrityksen palveluilla tarkoitettaan sen tuottamia palveluita, joiden toimimattomuus aiheuttaisi todennäköisesti tulon menetystä. Tietojärjestelmillä tarkoitetaan esimerkiksi tietokantoja ja rekistereitä. Tietoaineistoilla tarkoitetaan paperia, sekä ulkoisia tallennusmedioita, kuten USB-tikkut. Tietoon vaikuttavat ohjelmistoissa ilmenevät ongelmat, fyysiset ongelmat vaikuttavat suoraan tietoon tai vaikutus tulee ohjelmistojen kautta. Ongelmat palveluissa voivat vaikuttaa laitteiden ja työntekijöiden toimintaan. (Harju 2010, 23.) Suojattavat kohteet voidaan jaotella kuten taulukossa 2.

Taulukko2. Kohteiden jaotteleminen (ISO/IEC 207002; ISO/IEC 17799 2000)

	Kuvaus
Tieto	Tietokannat, tiedostot, sopimukset, asiakirjat, ohjeistukset, suunnitelmat, arkistoidut tiedot
Ohjelmistot	Apuohjelmat, kehitystyökalut, ohjelmistot, käyttöjärjestelmät
Fyysiset kohteet	Ulkoiset tallennusmediat, palvelimet, puhelimet, kannettavat, verkko- ja tietoliikennelaitteet
Palvelut	Sähkö, tietoliikennepalvelut, lämmitys, ilmastointi
Ihmiset	Työntekijät (osaaminen ja kokemus)
Aineettomat asiat	Yrityksen maine ja imago

4.2 Tiedon luokitteleminen

Tiedot olisi hyvä luokitella eri tasoihin, jotta tietoa olisi helpompi käsitellä ja hallinnoida. Taulukko 3. on yksi malli luokitella tietoa yrityksessä. Julkinen tieto voidaan julkaista missä tahansa, ja sen jakamisen tarkoitus on välittää julkista tietoa yrityksestä. Sisäinen tieto on tarkoitettu ainoastaan yrityksen sisäiseen käyttöön, eikä se kuulu ulkopuolisille tahoille. Sisäinen tieto ei kuitenkaan sisällä mitään luottamuksellista informaatiota. Luottamuksellinen ja salainen tieto voivat tarkoittaa pienissä yrityksissä samaa asiaa. Luottamuksellisen tai salaisen tiedon paljastuminen ulospäin voi aiheuttaa yritykselle rahallista menetystä tai jopa oikeudellisia ongelmia, sekä vaikuttaa yrityksen imagoon ja maineeseen. (Laaksonen ym. 2006, 161).

Taulukko3. Tiedon luokittelu ja paljastumisen vaikutukset (Tietoturvaopas 2010).

Luokittelu	**Paljastumisen seuraus**
Julkinen tieto	Hyötyä yritykselle
Sisäinen tieto	Ei juurikaan vaikutusta
Luottamuksellinen tieto	Haittaa yritykselle
Salainen tieto	Suurta haittaa yritykselle

Tiedon luokitteluun kuuluu myös tiedon hävittämisen kuvaus. Yrityksessä työskentelevien on tärkeää tietää miten tarpeettomaksi muuttunut tieto hävitetään, eli siis mitä dokumentteja saa heittää roskiin ja mitä tietoa on tuhottava tietoturvajätteen kautta. Tiedon hävittäminen koskee myös laitteistoa, esimerkiksi käytöstä poistetun kannettava kiintolevy on tuhottava fyysisesti, pelkkä tiedon pyyhkimi-

nen levyltä ei riitä. Sama koskee myös ulkoisia tallennusmedioita, kuten USB-tikkua tai ulkoista kiintolevyä. (Laaksonen ym. 2006, 161)

4.3 Tietoturvan tavoitetaso

Tietoturvan tavoitetaso vaihtelee eri yrityksissä, riippuen koosta, toimialasta ja ennen kaikkea käsiteltävän tiedon tärkeydestä ja luottamuksellisuudesta. Jokainen yritys joutuu hyväksymään, että täydellistä tietoturvaa on mahdoton toteuttaa. Varsinkin pienemmissä yrityksissä tietoturvan toteuttaminen on usein kiinni kustannuksista. Korkeatasoisen tietoturvan toteuttaminen vaatisi usein myös yrityksen toimintaan vaikuttavia muutoksia. Siksi kaikkea ei voida tai haluta muuttaa. Muutosprosessi voisi vaatia isojakin resursseja, jotta tietoturva saataisiin korkeatasoiseksi. Varsinkin pienemmissä yrityksissä käytetään usein kustannustehokasta tietoturvaa. Tässä mallissa tietoturva rakennetaan järkevin perustein, keskittyen vain olennaisiin uhkiin ja olennaisen tiedon suojaamiseen. Uhkien hyväksyminen tulee myös kysymykseen, jos todetaan, että uhkalle ei voida tehdä mitään tai siitä koituva haitta on hyvin pieni. Toteutunut tietoturva voi erota paljonkin määritetystä tavoitetasosta, jos ilmenee odottamattomia ongelmia resurssien tai yrityksen toimintojen muuttamisen kanssa. (VTT 2009.)

5 TIETOTURVAKARTOITUS KOHDEYRITYKSELLE

Tässä luvussa esitellään teoriaan pohjautuva tietoturvakartoitus kohdeyritykselle. Läpikäytäviä asioita ovat suojattavat kohteet, tiedon luokittelu, tietoturvan tavoite taso.

5.1 Suojattavat kohteet kohdeyrityksessä

Kuten luvussa 3.1 Suojattavat kohteet sanotaan, on ensin selvitettävä Yritys X:lle tärkeimmät suojattavat kohteet. Toteutin listan kyselemällä yrityksen työntekijöiltä, mitä tietoja he tarvitsisivat päivittäisessä työssään ja aiheuttiko tietojen puuttuminen ongelmia. Seuraavaksi oli selvitettävä missä tiedot sijaitsivat, sekä miten tiedot oli suojattu. Taulukko 4 on listattuna tiedot, jotka ovat yritykselle tärkeitä. Tämä ratkaisu tuntui tehokkaimmalta siksi, että yritys on kooltaan pieni, sekä järjestelmät ja toiminnot ovat hyvin yksinkertaisia. Tällä ratkaisulla säästettiin aikaa, sekä kokonaisuus oli helpommin hahmotettavissa.

Taulukko 4 Yrityksen suojattava tieto, sijainti ja pääsy tietoon.

Suojattava tieto	Sijainti	Pääsy tietoon
Asiakasrekisteri ja kassa järjestelmä	Palvelin, Varmuuskopio palvelimesta	Tunnus / salasana Yrityksen sisäinen verkko / VPN
Asiakasrekisteri tiedot	Palvelin, Varmuuskopio palvelimesta	Tunnus / salasana Yrityksen sisäinen verkko / VPN
Muut dokumentaatiot	Palvelin, Varmuuskopio palvelimesta	Tunnus / salasana Yrityksen sisäinen verkko / VPN
www-sivut	Ulkoistettu palvelin	Tunnus / salasana
Sopimukset	Paperiversiot, kaapissa	Lukittu kaappi
Henkilökunnantiedot	Taloushallinto järjestelmässä, kaapissa	Tunnus / salasana Yrityksen sisäinen verkko / VPN / Lukittu kaappi
Sähköposti	Ulkoistettu palvelin	Tunnus / salasana, miltä tahansa laitteelta
Kirjanpito	Palvelin, ulkoinen järjestelmä, kassaholvi	Tunnus / salasana Yrityksen sisäinen verkko / VPN, avain
Muut ulkoiset järjestelmät	Ulkoiset palvelimet	Tunnus / salasana, miltä tahansa laitteelta

5.2 Tiedonluokittelu kohdeyrityksessä

Kohde yrityksessä pelkkä tiedon perus luokittelu ei riitä (3.2 Tiedonluokittelu, taulukko 4.) vaan luottamuksellisen ja salaisen tiedon luokittelua on tarkennettu niin, että jokaiseen dokumenttiin on määritelty erikseen nimeämällä henkilöt, ketkä tietoa yrityksessä saavat käsitellä. Tällöin voidaan varmistua siitä, että tieto pysyy tarkasti rajattujen henkilöiden tiedossa. (Tietoturvaopas 2010.)

Kohdeyrityksessä ainoastaan julkista tietoa sisältävät dokumentit voidaan hävittää roskakorin kautta. Kaikki muut dokumentit tuhotaan tietoturvajätteen kautta. Työntekijöitä on myös ohjeistettu hävittämään dokumentit, joista eivät ole varmoja tietoturvajätteen kautta. Digitaalisten medioiden osalta yritys käyttää ohjeistusta, että tallennusmedia on aina tuhottava fyysisesti, niin että tieto ei ole enää luettavissa, eikä palautettavissa.

5.3 Tietoturvan tavoitetaso kohdeyrityksessä

Kuten luvussa 3.3 tietoturvan tavoitetaso todetaan, että yrityksen on hyvä määrittää itselleen tavoitetaso tietoturvan osalta. Yritys X tapauksessa päädyimme asettamaan tavoite tasoksi pyrkimyksen minimoimaan tietoturvaonnettomuudet. Myös tietoturvariskien toteutumistodennäköisyys pyritään pitämään mahdollisimman epätodennäköisenä, sekä että onnettomuuksista selvittäisiin nopeasti ja suurella todennäköisyydellä. Järjestelmät, jotka käyttävät suojattavia tietoja, sekä yrityksessä käytettävät toimintatavat eivät saa aiheuttaa riskejä, joiden toteutuminen olisi todennäköistä. Tätä pyritään estämään esimerkiksi uusimmilla järjestelmäversioilla, sekä pitämällä tarvittavia suojaustasoja yllä. Yrityksen tulee myös pitää huolta siitä, että henkilöstön osaaminen tietoturvasta on riittävällä tasolla, sekä että kaikki noudattavat tietoturva ohjeistusta.

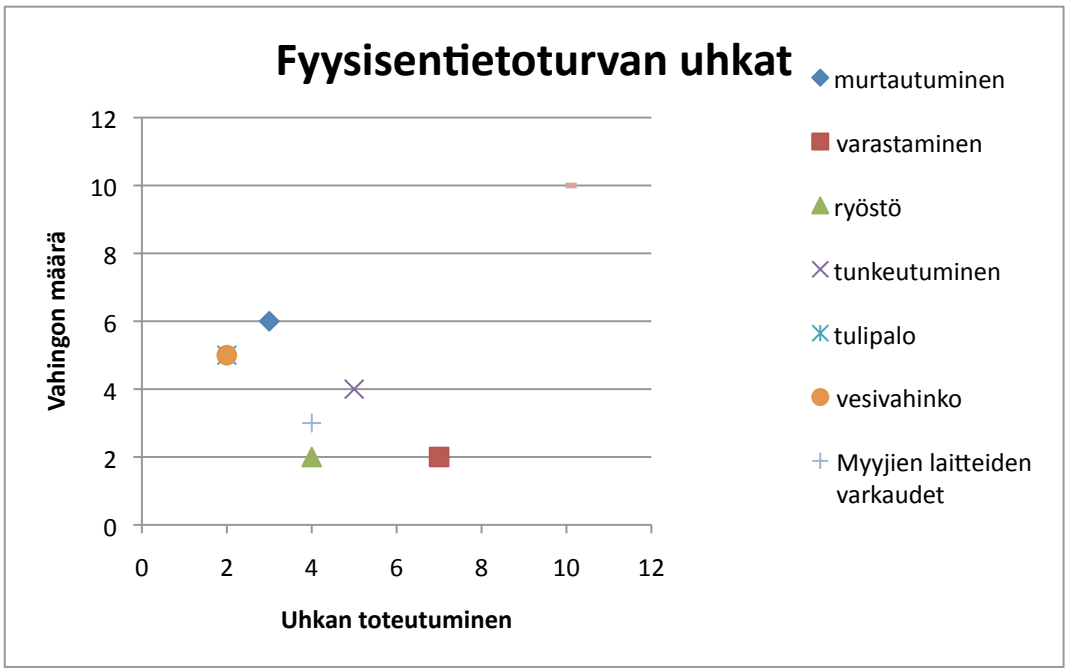
5.4 Tietoturva uhkat kohdeyrityksessä

Kun tiedetään mitä suojataan, miten tieto luokitellaan, sekä määriteltiin tietoturvan tavoitetaso. Voidaan alkaa selvittämään, tietoturvan eri osa-alueiden todelliset uhkat ja miten niiden toteutumista voidaan estää. Kohden yrityksessä läpikäytävät osa-alueet ovat, fyysinentietoturva, laitteistoturvallisuus, ohjelmistoturvallisuus, henkilöstöturvallisuus, sekä tietoliikenneturvallisuus. Riskien määrittelyyn tulen käyttämään jo aikaisemmin luvussa 3.1.1 mainitsemaani nelikettäriskianalyysia. Päädyin tähän mittariin, koska se on tehokas tapa arvioida riskin toteutumisen todennäköisyys ja riskin aiheuttaman haitan määrä, sekä eri riskit ovat nopeasti vertailtavissa keskenään. Riskejä arvioimassa kanssani oli yrityksen johto, joka tietää yrityksen nykytilasta eniten ja pystyy arvioimaan, mikä uhkista on todennäköisin ja mikä uhka aiheuttaa eniten haittaa toteutuessaan. Kehitysehdotukset perustuvat haastatteluun ja yrityksen päivittäisen toiminnan tarkkailuun tietoturvan osalta. (Miettinen 1999, 58.)

5.4.1 Fyysinen tietoturva

Yrityksen toimitilojen, sekä niissä sijaitsevien laitteiden suojaamista kutsutaan yleisesti nimellä fyysinen tietoturva. Se pitää myös sisällään palo-, vesi- ja sähkövauriot. Sekä inhimilliset uhkat, kuten varkaudet ja ilkivalta (Miettinen 1999, 19.)

Kuvio 3. havainnollistaa miten yritys on arvioinut fyysisen tietoturvallisuuden riskit. Kuvan horisontaalijana kertoo uhkan toteutumisen todennäköisyyden asteikolla 0-10, 0 = pienin mahdollinen todennäköisyys, 10 = suurin mahdollinen todennäköisyys. Vertikaalijana kertoo uhkan toteuttaman vahingon määrän, 0 = pienin mahdollinen vahinko, 10 = suurin mahdollinen vahinko.



Kuvio 3. Fyysisen tietoturvan uhkat kohde yrityksessä.

Tunkeutuminen

Yritys on suojannut fyysiset tilansa lukituksin, hälyttimin, sekä videovalvonnalla. Näitä voidaan pitää riittävänä toimena yrityksen fyysisen turvallisuuden kannalta. Kuitenkaan yrityksen sisällä tiloja jakavat ovet eivät ole lukittu. Tämä luo uhkan, siitä, että ulkopuolinen henkilö, voisi tunkeutumalla päästä yrityksen henkilökunnalle tarkoitettuihin tiloihin (Kuvio 3. tunkeutuminen). Esimerkiksi toimistoon, josta hän voisi saada käsiinsä yrityksen sisäistä tietoa.

Tunkeutumisen todennäköisyyttä riskitekijänä, voitaisiin vähentää merkittävästi tehostamalla kulun valvontaa ja asentamalla välioviin lukot. Sekä pitämällä ovia kiinni. (Miettinen 1999, 179-180.)

Varastaminen

Yrityksen päätoimiala on myynti ja yhtenä inhimillisenä uhkana voidaan pitää varkauksia (Kuvio 3. Varastaminen) yrityksen myymälässä. Yritys on pyrkinyt suojautumaan tätä vastaan varashälyttimillä demolaitteissa, erillisillä tuotelukoilla, sekä lukituilla lasikaapeilla. Yritys käyttää myös videovalvontaa tiloissaan. Kamera valvonnasta huolimatta, yritys on huomannut, että pienimpiä tuotteita varastetaan aika-ajoin ja se näkyy inventaarioissa.

Yritys pystyisi estämään varkauksista vielä osan asentamalla hälytin portit. Hälytysporteilla, voisi olla myös ennalta ehkäisevä vaikutus. Vaikka tuote varkaudet eivät sinänsä aiheuta yritykselle tietojen menetystä, ne joka tapauksessa aiheuttavat rahallista tappiota. Yrityksellä on vakuutus, joka kattaa varkaudet. Kuitenkaan useimmiten yksittäisen varastetun tuotteen arvo, ei ylitä omavastuu osuutta.

Palo, vesi ja sähkö vahingot

Kuten kuviosta 3 voidaan nähdä, palo-, vesi-, ja sähkövahingot ovat yrityksen näkemyksen mukaan mahdollisia, mutta hyvin epätodennäköisiä. Haitat usein jäävät hyvin pieniksi, johtuen yrityksen toimialasta. Palo- ja vesivahingot on ulkoistettu vakuutusyhtiölle.

Myyjien laitteiden varastaminen

Yritys on antanut myyjille käyttöön puhelimet. Usein päivän aikana nämä puhelimet ovat myymälän tiskillä ja siksi myyjien puhelimet (Kuvio 3 myyjien laitteiden varastaminen) ovat mahdollisia kohteita varkaille. Monesti puhelin saattaa jäädä myyntitiskille ilman valvontaa. Puhelimen varastamisesta ei välttämättä koidu yritykselle suurta tietoturva haittaa, koska puhelimet on suojattu pääsykoodilla. Puhelimen katoaminen voi kuitenkin aiheuttaa yritykselle pienen rahallisen tappion.

Yrityksen olisi hyvä ohjeistaa myyjiä, pitämään puhelimet tiskin alemmilla tasoilla tai taskussa, jotta varkaus tilanteilta vältyttäisiin. Puhelimiin tulisi myös ottaa käyttöön find my device-palvelu, siten ne voidaan tarvittaessa jäljittää, sekä etätyhjentää, jos puhelinta ei saada takaisin. (Apple iCloud)

Ryöstö

Ryöstön kohteena yritys ei ole hyvä, johtuen siitä, että myynneistä lähes 90% tehdään korttimyynteinä. Yritys pyrkii myös pitämään rahan määrän kassassa mahdollisimman pienenä. Isoimmat summat siirretään välittömästi pois kassasta myynti tapahtuman jälkeen. Edellä mainitulla toimenpiteellä pyritään minimoimaan rahallinen tappio. Yrityksellä on myös video valvonta ja useat kamerat kuvaavat kassatiskin läheisyyttä. Yrityksessä on ohjeistus työntekijöiden vähimmäislukumäärästä. Liikkeen aukioloaikana henkilöstöä täytyy olla vähintään kaksi, jotta myymälää voidaan pitää auki. Ryöstön todennäköisyyttä pidettiin suhteellisen pienenä, kuten kuviosta 3 on nähtävissä. Myös ryöstöstä koituva haitta on lähinnä rahallista.

Yrityksen kannattaisi kuitenkin harkita aikaviivelukolla varustettuja säiliöitä, joihin voitaisiin laittaa suurimmat setelit kassasta. Yrityksen kannattaisi myös asentaa kassa tiskille hälytysnäppäin, jota painamalla hälytys lähtisi vartioliikkeeseen. Henkilökunnan ohjeistaminen tilanteessa toimimiseen olisi varmasti yksi helpoimmin suoritettavista parannuksista.

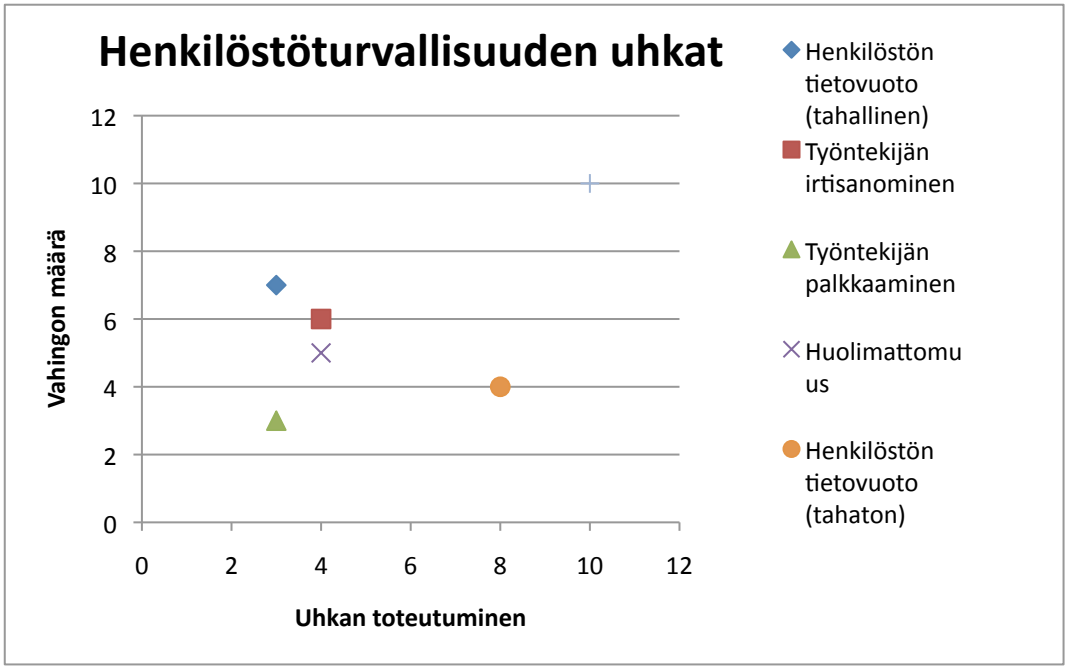
Murtautuminen

Yrityksen tilat ovat suojattu lukoilla, hälyttimillä, sekä videovalvonnalla. Kuten kuvasta 3 nähdään murtautumisen riskiä ei voida täysin estää. Yrityksen ei kuitenkaan kannata sijoittaa murtosuojaukseen enempää resursseja, koska riskistä aiheutuvat rahalliset vahingot on ulkoistettu vakuutus yhtiölle. On kuitenkin mahdollista, että murtautujat voivat saada mukaansa tietoja varastamistaan laitteista. Tiedon määrä itse laitteissa on vähäinen, siksi vahingon määrä jää vain keskitasolle. Yritys on pyrkinyt sijoittamaan tietonsa yrityksen omille, sekä ulkoistetuille palvelimille.

5.4.2 Henkilöstöturvallisuus

Henkilöstöturvallisuudella pyritään ehkäisemään henkilökunnan aiheuttamia tietoturvauhkia. Yrityksen palkatessa uusia henkilöitä olisi hyvä tarkastaa henkilön luotettavuus, taustat, sekä että hakijalla on riittävä osaaminen hakemaansa tehtävään. Velvollisuudet on tehtävä selväksi työsopimuksessa, joka palkattavan on hyväksyttävä. Vanhan työntekijän eroaminen on työn antajalle hankalatilanne monella tapaa. Työn antaja voi ottaa eronneelta työntekijältä kaiken yrityksen omaisuuden takaisin, kuten avaimet, laitteet ja poistaa tunnukset. Työnantaja ei kuitenkaan voi pyyhkiä eronneen työntekijän muistia. Tämä luo tietoturva uhkan. Työnkuvaan liittyen voidaan kuitenkin edellyttää salassapitosopimusta, jos henkilö käsittelee työssään materiaalia, joka on arkaluontoista tai muuten yrityksen toiminnan kannalta tärkeää. (ISO/IEC 27002; ISO/IEC 17799 2000; Laaksonen ym. 2006 139-142.)

Kuvio 4. Havainnollistaa, miten yritys on arvioinut henkilöstö turvallisuuden riskit. Kuvan horisontaalijana kertoo uhkan toteutumisen todennäköisyyden asteikolla 0-10, 0 = pienin mahdollinen todennäköisyys, 10 = suurin mahdollinen todennäköisyys. Vertikaalijana kertoo uhkan toteuttaman vahingon määrän, 0 = pienin mahdollinen vahinko, 10 = suurin mahdollinen vahinko



Kuvio 4. Henkilöstöturvallisuuden uhkat kohde yrityksessä.

Henkilöstön tietovuoto (tahaton)

Pitäessäni yrityksen johdon kanssa kokousta, jossa arvioimme yritykseen kohdistuvien uhkien todennäköisyyttä ja uhkan toteutuessa toteutuvaa vahingon määrää. Käsittelimme myös henkilöstö turvallisuuden osa-aluetta. Kuten kuviosta 4. Voidaan katsoa henkilöstön tahaton tietovuoto on yksi merkittävimmistä uhkista henkilöstöturvallisuuden puolella. Esimerkkinä voidaan pitää tilannetta, jossa työntekijä puhuu asiakkaalle sivulauseessa jotain tietoa, joka olisi tarkoitettu ainoastaan talon sisäiseen käyttöön. Haitta kuitenkin tässä tilanteessa ei välttämättä ole suuri, mutta vahinkoa on mahdollista syntyä.

Tahattoman tietovuodon ennaltaehkäisemiseksi yrityksen olisi hyvä ohjeistaa työntekijöitään, sekä myös muistuttaa asiasta aika-ajoin.

Henkilöstön tietovuoto (tahallinen)

Toiseksi suurimpana riskinä pidettiin henkilöstön tahallisesti aiheuttamaa tietovuotoa. Kuten kuviosta 4. voidaan todeta todennäköisyyttä tahallisen tietovuodon toteutumiseen pidettiin suhteellisen pienenä. Suurin riski milloin tämä voisi toteutua olisi, kun henkilö irtisanotaan yrityksen palveluksesta. Olisi mahdollista, että irtisanottu kertoisi yrityksen sisäistä tietoa, esimerkiksi kilpailevalle taholle. Tätä on pyritty estämään salassapitosopimuksella, jonka jokainen yritykseen palkattu työntekijä on joutunut allekirjoittamaan. On otettava huomioon, että kyseistä uhkaa on hyvin hankala poistaa tai estää tapahtumasta. Siksi yritys pyrkii salassapitosopimuksella ennaltaehkäisevään toimintaan. Sekä tietovuodon haitoista aiheutuneiden kulujen kattamiseen henkilöltä, joka on aiheuttanut tietovuodon.

Kuten yllä todettiin, ei tahallista tietovuodon uhkaa voida kokonaan pois sulkea. Yritys on sitouttanut kaikki työtekijänsä salassapitosopimukseen. Loppu riski yrityksen on käytännössä hyväksyttävä.

Työntekijän palkkaaminen

Yrityksen haastatellessa uusia työntekijöitä pyrkii yritys tarkastamaan henkilön taustat, sekä soveltuvuuden työtehtävään. Jos hakija on käyttänyt suosittelijoita ovat ne yksi tapa saada tietoa hakijan soveltuvuudesta. Jos hakija päätetään palkata hänen tulee allekirjoittaa työsopimus, sekä salassapitosopimus. Yrityksellä on myös tapana käyttää koeaikaa, jokaisen uuden työntekijän kohdalla. Näillä edellä mainituilla toimilla pyritään estämään, niin sanotun väärän henkilön palkkaamista yritykseen. Siksi uuden työntekijän palkkaamisesta aiheutuvia riskejä pidettiin hyvin pieninä kuten kuvio 4 osoittaa.

Yrityksen ei ole järkevää panostaa enempää resursseja työntekijän palkkaamiseen liittyvien uhkien ennaltaehkäisemiseen, kuin mitä se tällä hetkellä käyttää.

Työntekijän irtisanominen

Työntekijän irtisanominen yrityksessä tapahtuu aina kasvotusten. Irtisanotulta pyydetään yrityksen omaisuus takaisin. Esimerkiksi avaimet, puhelimet, muut laitteet, käyntikortit, sekä työasu. Irtisanotun kanssa käydään läpi hänen allekirjoittamansa salassapitosopimuksen velvoitteet, jotka koskevat yrityksen jälkeistä aikaa. Näillä toimilla pyritään estämään irtisanotun henkilön tuomaa uhkaa. Kuten kuviosta 4 käy ilmi, yrityksen johto piti kuitenkin työntekijän irtisanomista kohtuullisena uhkana. Juurikin siksi, että henkilön muistia ja tietotaitoa ei voida poistaa.

Yrityksen johto voisi parantaa tietoturvaa yksinkertaisella menetelmällä. Yrityksen johdon, olisi hyvä ilmoittaa välittömästi muille työntekijöille, että kyseinen henkilö ei ole enää yrityksen palveluksessa. Sekä Pyydettäessä yrityksen omaisuutta takaisin irtisanotulta henkilöltä, olisi kannattavaa poistaa hänen hälytyskoodit, sekä järjestelmätunnukset ja vaihtaa sähköpostin salasana. Tällä voitaisiin pienentää irtisanotun henkilön aiheuttamaa uhkaa entisestään.

Henkilöstön huolimattomuus

Kuvio 4 osoittaa, että henkilöstön huolimattomuus koettiin mahdolliseksi uhkaksi. Toteutuessaan tämä voisi aiheuttaa yritykselle haittaa. Esimerkiksi sähköpostin lähettäminen väärään osoitteeseen voisi aiheuttaa tietovuodon, joka voisi aiheuttaa pientä haittaa yritykselle. Yritys pyrkii ehkäisemään henkilöstön huolimattomuudesta johtuvia uhkia muistuttamalla henkilöstöä huolellisuudesta ja vastuullisuudesta.

Yritys on pyrkinyt estämään tämän uhkan niin tehokkaasti, kuin se on mahdollista. Käytännössä uhkan estämiseksi ei kannata panostaa enempää resursseja.

Avainhekilöt

Yritys on riippuvainen muutamasta työntekijästä, joita voidaan kutsua avainhenkilöiksi. Heidän erikoisosaaminen on yrityksen toiminnan kannalta tärkeää. Jos henkilöt jostain syystä menehtyisivät tai lähtisivät yrityksen palveluksesta. Olisi mahdollista, että yritys joutuisi miettimään koko toimintansa uudelleen. Kyseisiä henkilöitä on hyvin hankala korvata, koska samaa osaamista ja certifiointeija omaavia henkilöitä on hyvin vaikea löytää suomesta. Tämä asettaa yrityksen hyvin hankalaan asemaan. (Miettinen, 1999, 171-172.)

Siksi yrityksen olisi hyvä kouluttaa myös muuta henkilöstöään kyseisiin certifiointeihin. Näin voitaisiin välttää, esimerkiksi avainhenkilöiden pitkistä sairauslomista aiheutuvat ongelmat.

Henkilöstön tietoturva tietämyksen taso

Nelikenttä analyysin lisäksi tein henkilöstölle yhdeksän kysymystä käsittävän kyselyn tietoturvasta. Kysely toteutettiin paperi versiona, johon henkilöillä oli yksi päivä aikaa vastata. Kysymyksillä on tarkoitus kartoittaa, millainen tietämys henkilöstöllä on tietoturvasta. Ne ovat tasoltaan yleisluotoisia kysymyksiä tietoturvasta. Kysymyksiin onnistuneesti vastaaminen ei vaadi syvää tietämystä tietoturvasta.

Ensimmäinen kysymys mittaa henkilöiden tietämystä, miten he käsittävät vahvan salasanan. Kysymys itsessään kuuluu seuraavasti: Kerro millainen on vahva salasana?

Henkilöstöstä kaikilla oli tietämys, mitä vaaditaan vahvan salasanan luomiseksi. Yllätyksenä voidaan kuitenkin pitää yhtä poikkeavaa vastausta, jossa mainittiin, että alle 20 merkin salasana ei ole turvallinen ja on murrettavissa. Suurin osa henkilöstöstä oli vastannut salasana standardin mukaan. Vahva salasana vaatii vähintään 8 merkkiä, vähintään yksi iso kirjain, yksi numero. Kaikki myös mainitsivat, ettei salasana saisi olla esimerkiksi, lapsen nimi, koiran nimi, syntymäaika tai vas-

taava. Voidaan siis todeta, että henkilöstö oli hyvin tietoinen, miten salasana tulisi muodostaa.

Toisena kysymyksenä henkilöstöltä kysyttiin: Onko seuraava väittämä totta? Jotta muistaisin salasanani, voin käyttää samaa salasanaa kaikissa kohteissa. Perustele vastauksesi.

Henkilöstöstä yksi vastasi, että samaa salasanaa voidaan käyttää kaikissa palveluissa. Muut henkilöstöstä vastasivat, että samaa salasanaa ei tulisi käyttää muissa palveluissa, sekä jokaisessa palvelussa tulisi käyttää yksilöllistä salasanaa, eikä muunnosta yhdestä ainoasta salasanasta. Vastausten perustella voidaan sanoa, että henkilöstöstä suurin osa ymmärsi, ettei saman salasanan käyttäminen useassa palvelussa ole kannattavaa. Se nostaa tietoturvauhkan toteutumista ja mahdollista haitan määrää moninkertaiseksi.

Kolmannessa kysymyksessä henkilöstöltä kysyttiin: Miten toimit työssäsi tulosteiden kanssa, joita ei tarvita. Niiden sisältäessä esimerkiksi asiakastietoja?

Kaikki henkilöstöstä vastasivat hävittävänsä tulosteet tietoturvajätteen kautta. Yritys on panostanut tietoturvajätteen keräysastioihin. Yrityksen johto on myös ohjeistanut henkilöstöä käyttämään tietoturvajätettä, myös silloin kun henkilö ei ole varma kuuluuko paperi tietoturvajätteeseen vai ei. Vastausten perusteella voidaan todeta, että henkilöstö käyttää tietoturvajätettä tehokkaasti ja ohjeistuksen mukaan. Yritys on siis saavuttanut tavoitteensa.

Neljäntenä kysymyksenä henkilöstöltä kysyttiin: Onko seuraava väittämä totta? Kun alustat muistitikun, tietoja ei voida enää palauttaa. Perustele vastauksesi.

Henkilöstöstä suurin osa vastasi, että väite ei pidä paikkaansa, ja että tiedot on mahdollista palauttaa erinäisin menetelmin. Ainoastaan yksi henkilöstöstä ei ollut tietoinen, onko väite totta vai ei. Vastausten perusteella voidaan todeta, että henkilöstöstä suurin osa ymmärtää, että muistitikun alustaminen ei poista tietoa tallennus mediasta lopullisesti.

Viidentenä kysymyksenä henkilöstöltä kysyttiin: Onko seuraava väittämä totta? Kun haluat poistaa tiedoston koneelta, heität tiedoston roskakoriin ja tyhjennät roskakorin. Tiedostoa ei voida enää palauttaa roskakorin tyhjennyksen jälkeen. Perustele vastauksesi.

Henkilöstöstä yhtä lukuun ottamatta, kaikki olivat tietoisia, että tiedosto ei poistu koneesta lopullisesti tyhjentämällä roskakorin. Osa vastaajista toi esiin myös, että tieto on palautettavissa, vaikka levy tyhjennettäisiin tai ylikirjoitettaisiin. Vastausten perusteella voidaan sanoa, henkilöstön olevan tietoinen, että kiintolevylle tallennettua tietoa, ei voi tuhota heittämällä tiedostot roskakoriin ja tyhjentämällä sen.

Kuudentena kysymyksenä henkilöstöltä kysyttiin: Onko seuraava väittämä totta? Kun näytät asiakkaalle tietoja koneen näytöltä on varottava, ettei hän näe muita hänelle kuulumattomia tietoja. Perustele vastauksesi.

Henkilöstöstä kaikki pitivät väittämää totena. Yksi vastaajista kuitenkin kertoi, että asiakkaalle ei saisi näyttää koneen ruutua, jos kone sisältäisi tietoa, jota asiakas ei saisi nähdä. Vastausten perusteella voidaan siis sanoa henkilöstön ymmärtävän, että ylimääräinen tieto, joka ei koske asiakasta on piilotettava ruudulta pois, kun havainnollistetaan asiakkaalle näytöllä jotain.

Seitsemäntenä kysymyksenä henkilöstöltä kysyttiin: Yrityksen tiloihin tulee henkilö, joka kertoo olevansa hälytinlaitteiden korjaaja. Miten varmistut, että henkilö on se kuka hän sanoo olevansa?

Kaikki henkilöstöstä olisivat toimineet perus periaatteeltaan samoin. Jokainen vastaaja, olisi pyrkinyt todentamaan henkilön identiteettiä, sekä sen missä yrityksessä hän työskenteli. Seuraavaksi he olisivat selvittäneet yrityksen johdolta, onko hälytinlaitteille tilattu korjaajaa. Toimintatapaa voidaan pitää oikeana. Henkilöstö olisi näin varmistanut, ettei väärä henkilö pääsisi käsiksi yrityksen hälytysjärjestelmään.

Kahdeksantena kysymyksenä henkilöstöltä kysyttiin: Pidätkö tietoturvaa tärkeänä asiana? Perustele vastauksesi.

Yhtä henkilöä lukuun ottamatta kaikki vastasivat pitävänsä tietoturvaa tärkeänä asiana, varsinkin työssään. Ainoastaan yksi vastaajista piti tietoturvaa yliarvostettuna ja aivan liian paljon huomio arvoa saavana, sekä arkea vaikeuttavana tekijänä. Vastausten perusteella voidaan siis todeta, että suurin osa suhtautui tietoturvaan vakavasti ja asiaan kuuluvalla tavalla. Kuitenkin yksi henkilö voi huolimattomuudellaan ja asenteella aiheuttaa yritykselle tietoturvauhkan.

Yhdeksäntenä kysymyksenä henkilöstöltä kysyttiin: Haluaisitko saada enemmän tietoa ja ohjeistusta tietoturvasta, sekä yrityksen tietoturva politiikasta?

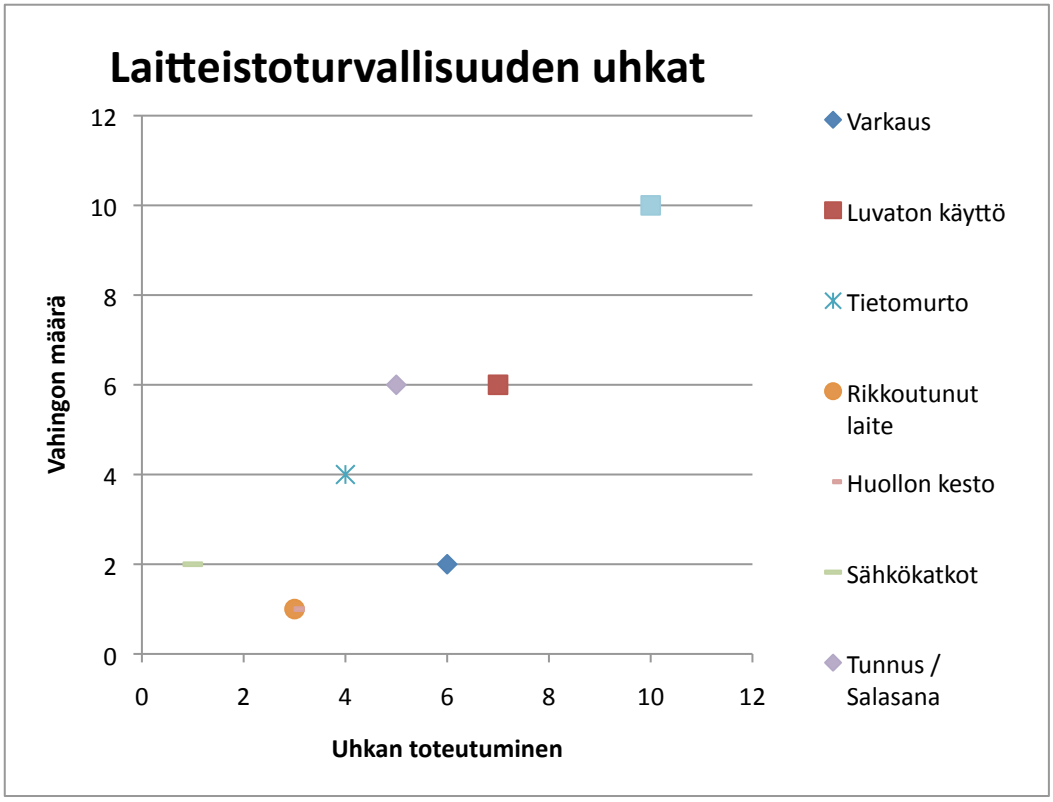
Voidaan pitää yllättävänä, että henkilöstöstä ainoastaan kaksi halusi saada enemmän tietämystä ja ohjeistusta. Muut henkilöstöstä kokivat tietävänsä tarpeeksi tai eivät muuten olleet kiinnostuneita.

Yhteenvetona voidaan todeta, että henkilöstöllä on suhteellisen hyvä perustietämys tietoturvasta. Kuitenkin yhden henkilön välinpitämättömyys ja negatiivinen asenne tietoturvaa kohtaan voi aiheuttaa turhan tietoturvariskin. Henkilön asennetta tietoturvaa kohtaan voi olla hyvin hankala muuttaa. Siitä huolimatta yrityksen tulisi motivoida ja kannustaa kaikkia työntekijöitä huolehtimaan tietoturvasta.

5.4.3 Laitteistoturvallisuus

Laite turvallisuudella tarkoitetaan yrityksen omistamien fyysisten laitteiden, kuten tietokoneiden, tablet-laitteiden, puhelimien turvallisuutta. Tavoite on estää laitteiden vahingoittuminen, häviäminen, varkaus, sekä muut laitteiden kautta yritykseen haitallisesti liittyvät tapahtumat. Yrityksen kannattaa selvittää, mitä laitteita heillä on käytössään ja millaisia suojausmenetelmiä laitteet tarvitsevat. Yrityksen johdon olisi hyvä määritellä erilaitteille käyttöpolitiikka. Esimerkiksi, jos työnantaja tarjoaa alaiselleen tietokoneen ei työntekijällä pitäisi olla tarvetta käyttää omaa konetta työssään. Jokainen ylimääräinen laite aiheuttaa riskin tietoturvalle. Esimerkiksi työntekijän omassa koneessa voi olla tietoturva-aukko, jota voitaisiin hyödyntää yrityksen tietoihin pääsemiseksi. Laitteiden tietoturvaan vaikuttaa myös laitteiden sijainti. Yrityksen on hyvä suojata laitteensa varkauksien ja muiden fyysisten uhkien kannalta. Koneita ei siis kannata sijoittaa lähelle poistumisteitä tai jättää yleisiin tiloihin valvomatta. Koneet, joita työntekijät kuljettavat mukanaan yrityksen toimitilojen ulkopuolella, ovat suuremmassa riskissä joutua varastetuksi tai kadota. Siksi on tärkeää, että yritys kryptaisi jokaisen laitteen kiintolevyn, sekä ulkoiset tallennus mediat, ennen kuin niitä liikutellaan yrityksen tiloista. On huolehdittava, että koneissa on vahvat tunnukset, sekä salasanat. Liikuteltavissa laitteissa on hyvä käyttää find my device toimintoa, jolla voidaan paikantaa laite ja hallinnoida sitä etänä, sekä tarvittaessa poistaa etäkomennolla laitteen sisältö. (Laaksonen ym. 2006, 126; ISO/IEC 27001 2005; Apple iCloud 2012)

Kuvio 5. havainnollistaa miten yritys on arvioinut laitteistoturvallisuuden riskejä. Kuvan horisontaalijana kertoo uhkan toteutumisen todennäköisyyden asteikolla 0-10. 0 = pienin mahdollinen todennäköisyys, 10 = suurin mahdollinen todennäköisyys. Vertikaalijana kertoo uhkan toteuttaman vahingon määrän. 0 = pienin mahdollinen vahinko, 10 = suurin mahdollinen vahinko.



Kuvio 5. Laitteistoturvallisuuden uhkat kohde yrityksessä.

Luvaton käyttö

Kuten yllä olevasta kuviosta 5 on nähtävissä, yrityksen johto koki laitteistoturvallisuuden suurimmaksi riskiksi, luvattoman käytön. Luvattomalla käytöllä tarkoitetaan, että laitetta käyttää henkilö, kenellä ei ole lupa käyttää laitetta. Usein tällainen henkilö pyrkii saamaan itselleen informaatiota, yrityksen järjestelmästä tai paikallisesti koneelta. Yritys pyrkii estämään tämän tunnus ja salasana kyselyllä. Laite siis kysyy aina tunnusta ja salasanaa kun konetta halutaan käyttää.

Yritys voisi parantaa tietoturvaa yksinkertaisella toimenpiteellä asettamalla koneet tekemään lokitiedostoa. Näin voidaan jälkeenpäin määrittää, mitä mahdollisesti on tapahtunut.

Tunnus ja salasana

Toiseksi suurimpana uhkana laitteistoturvallisuudessa yrityksen johto piti kuvion 5 mukaisesti tunnus ja salasana käytäntöä. Tunnuksilla pääsee niin palvelimelle, kuin yrityksen sisäisiin järjestelmiin. Tunnusten ja salasanojen paljastuessa, voisi se aiheuttaa vakavan tieturvaongelman. Yritys on kuitenkin pyrkinyt estämään uhkan toteutumista, antamalla jokaiselle työntekijälle omat tunnukset ja salasanat. Käyttäjä on myös pakotettu vaihtamaan salasanansa määräajan välein. (Miettinen, 1999, 235-236.)

Muistuttamalla aika ajoin työtekijöitä turvallisen salasanan merkityksestä, yritys voisi parantaa tietoturvaansa tämän uhkan osalta.

Tietomurto

Tietomurron mahdollistaa usein haittaohjelma tai aukko käyttöjärjestelmän tai ohjelmiston versiossa. Uhkana tietomurtoa pidettiin keskitasolla ja sen aiheuttama haitta olisi keskiluokkaa. Tämä käy ilmi myös kuviosta 5. Yritys pyrkii estämään kyseisen uhkan toteutumisen päivittämällä järjestelmänsä ja ohjelmistot uusimpaan mahdolliseen versioon, aina uuden version ilmestyessä. Myös tietomurron osalta, yritys arvioi jatkuvasti tilannetta uudelleen, jos epäilyksiä herää voidaan tarvittaessa hankkia virustorjunnat, sekä muut erikoisohjelmistot.

Laitteiden rikkoutuminen

Kuten kuvio 5 osoittaa laitteiden rikkoutuminen ei ole yritykselle suuri uhka, koska laitteisto on nopeasti korvattavissa ja koneista on ajan tasalla olevat varmuuskopiot. Yrityksellä on myös toimiva huolto, jossa laitteet voidaan nopeasti huoltaa toimintakuntoon. Jos laitteita hävitetään tai laitteiden tallennus medioita joudutaan vaihtamaan tuhoaa yrityksen huolto fyysisesti kyseiset mediat.

Yritys voisi pyrkiä pitämään yksittäisiä laitteita varalla, jotta laiterikkojen aikana voitaisiin nopeasti ottaa käyttöön varalaite. Ennen kuin alkuperäinen laite korjataan tai korvataan uudella.

Sähkökatkot

Sähkökatkot yrityksen tiloissa eivät ole yleisiä ja siksi niitä pidetään hyvin epätodennäköisenä uhkana. Sähkökatkot harvoin aiheuttavat suurta haittaa yritykselle. Tämä käy ilmi myös kuvasta 5. Yrityksen tärkeimmät koneet ovat suojattu UPS-järjestelmillä, jolloin ne saavat virtaa lyhyiden sähkökatkojen ajan. Pidemmissä sähkökatkoksissa UPS-järjestelmä ajaa laitteet alas, jos UPS:in akun teho heikkenee liikaa. Pitkien sähkökatkojen osalta, yrityksen on vain hyväksyttävä sen aiheuttamat haitat.

Varkaus

Laitteiden varkautta pidettiin todennäköisenä, varsinkin liikuteltavien laitteiden osalta. Kuviosta 5 ilmenee, kuinka varkaudesta aiheutuneiden haittojen määrä arvioitiin hyvin pieneksi, johtuen koneen kiintolevyn kryptauksesta, sekä tunnus ja salasana politiikasta, joilla pyritään estämään laitteen käyttö tai sieltä tiedon saaminen. Yritys on ohjeistanut pitämään tiedon määrän koneissa mahdollisimman pienenä paikallisesti. Tarkoituksena on siis pitää pääsy tietoihin ainoastaan etäyhteyden kautta palvelimelle. Tieto ei siis ole suoraan laitteella, vaan palvelimella. Laite on ainoastaan yhteyden muodostamista varten, jotta tietoon päästään tarvittaessa käsiksi. Tällä pyritään vähentämään tiedon menetyksen määrää, jos laite esimerkiksi varastetaan. (Laaksonen, 2006, 168-169.)

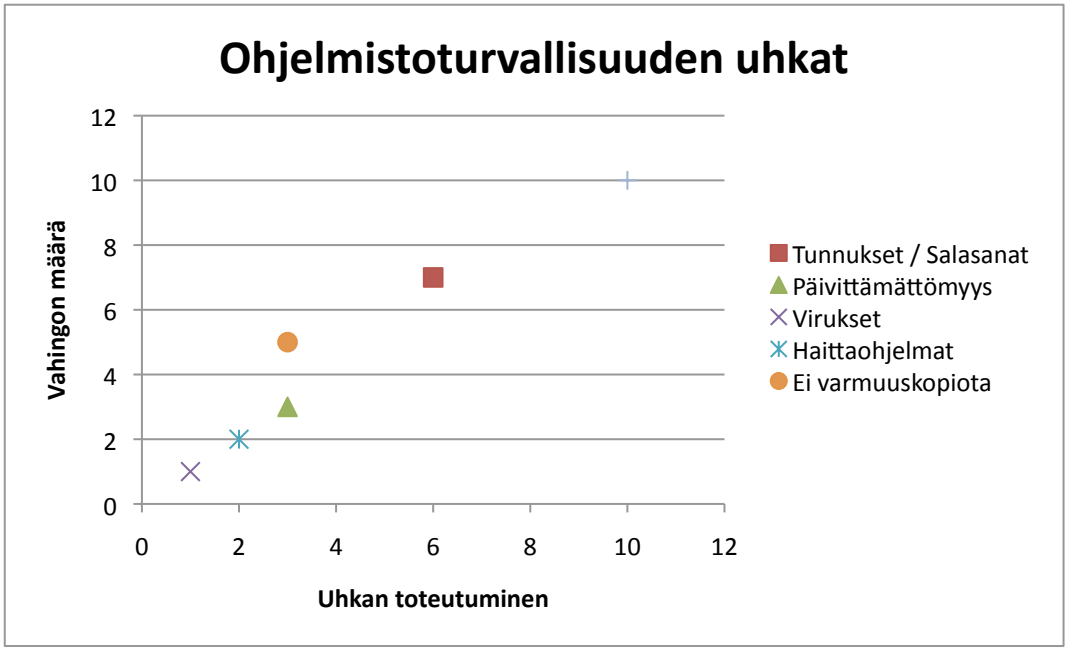
Yrityksen olisi silti hyvä harkita find my device palvelun käyttöönottoa, jotta varastetut laitteet voitaisiin jäljittää tai tarvittaessa tyhjentää etäyhteydellä. Tämä parantaisi yrityksen tietoturvaa varkaus tilanteissa huomattavasti. (Apple iCloud 2012)

5.4.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus pitää sisällään ohjelmisto lisenssien ja ohjelmistojen hallintaa. Ohjelmiston koodissa olevat virheet voivat aiheuttaa tietoturva-aukkoja. Riskiä kuitenkin voidaan vähentää, päivittämällä ohjelmistoa säännöllisesti. On myös mahdollista, että väärin asetetut asetukset aiheuttavat tietoturva-aukkoja. Työ asemille ei ole suositeltavaa asentaa ohjelmia, joita ei työkäytössä tarvita. Työnkannalta turhat ohjelmistot voivat aiheuttaa turhia tietoturva-aukkoja, sekä ne usein laskevat työntuottavuutta. (Miettinen, 1999, 225-226; Ruohonen, 2002, 4; ISO/IEC 27002;ISO/IEC 17799 2000.)

Yrityksessä käytetään koneina ainoastaan Mac OS X, sekä iOS alustaisia laitteita. Kyseisissä käyttöjärjestelmissä ei ole tarvetta virustorjunnalle, koska järjestelmä on unix pohjainen. Yrityksellä on käytössään useita erikoisohjelmistoja, jotka ovat isojen ja tunnettujen ohjelmistotalojen tuottamia ja siksi ne ovat turvallisia vaihtoehtoja. (Apple Mac OS X Mountain Lion 2012)

Kuvio 6. Havainnollistaa, miten yritys on arvioinut ohjelmistoturvallisuuden riskejä. Kuvan horisontaalijana kertoo uhkan toteutumisen todennäköisyyden asteikolla 0-10. 0 = pienin mahdollinen todennäköisyys, 10 = suurin mahdollinen todennäköisyys. Vertikaalijana kertoo uhkan toteuttaman vahingon määrän. 0 = pienin mahdollinen vahinko, 10 = suurin mahdollinen vahinko.



Kuvio 6. Ohjelmistoturvallisuuden uhkat kohde yrityksessä.

Tunnukset ja salasanat

Ohjelmistoturvallisuuden suurimpana uhkana yritys koki olevan, tunnusten ja salasanojen joutuminen ulkopuoleisen tahon tietoisuuteen. Kuten kuvio 6 osoittaa uhkan toteutuminen koettiin olevan mahdollinen, sekä toteutuessaan sen aiheuttamat haitat ovat suuret. Yrityksellä on useita eri tunnuksia, myös ulkoisille palvelimille. Esimerkiksi sähköpostipalvelimen tunnusten joutuminen ulkopuoleisen tahon tietoisuuteen, voisi aiheuttaa vakavan tietovuodon. Yritys pyrkii estämään uhkan toteutumista, luomalla työntekijöille omat tunnukset ja salasanat. Käyttäjät ovat myös pakotettuja vaihtamaan salasanaa määräajan välein. (Miettinen, 1999, 235-236.)

Muistuttamalla aika ajoin työtekijöitä turvallisen salasanan merkityksestä, yritys voisi parantaa tietoturvaansa tämän uhkan osalta.

Päivittämättömyys

Yrityksellä on useita koneita, sekä useita eri ohjelmistoja. Koneiden ohjelmistoja pyritään päivittämään aina, kun mahdollista. Tämä ei kuitenkaan läheskään aina tapahdu välittömästi, uuden päivityksen ilmestyttyä. Siksi se luo myös potentiaalisen tietoturva-aukon, kuten kuvio 6 osoittaa.

Yrityksen olisi hyvä automatisoida päivitykset, jokaiseen yrityksen koneeseen. Aina kun uusin ohjelmisto versio julkistetaan, se latautuisi automaattisesti koneelle. Näin parannettaisiin yrityksen ohjelmistotietoturvantasoa.

Virukset

Kuten kuvio 6 osoittaa, viruksia yrityksen johto ei pitänyt merkittävänä uhkana. Johtuen siitä, että yrityksen kaikki koneet ja laitteet ovat Mac OS X tai iOS pohjaisia. Järjestelmät ovat tunnetusti vapaita virus ongelmista. Yritys kuitenkin arvioi jatkuvasti tilannetta uudelleen, tämän uhkan osalta, jos epäilyksiä herää voidaan tarvittaessa hankkia virustorjunnat, sekä muut erikoisohjelmistot. (Apple Mac OS X Mountain Lion 2012)

Haittaohjelmat

Haittaohjelmia pidettiin yrityksessä uhkana, koska haitta ohjelmia on esiintynyt myös Mac OS X ympäristössä. Kuitenkin uhka oli hyvin pieni, kuten kuvio 6 osoittaa. Applen tarjoamien nopeiden päivityksien ansiosta, joka paikkaa ohjelmisto aukot. Yritys kuitenkin arvioi jatkuvasti tilannetta uudelleen tämän uhkan osalta, jos epäilyksiä herää voidaan tarvittaessa hankkia virustorjunnat, sekä muut erikoisohjelmistot. (Apple Mac OS X Mountain Lion 2012)

Ei varmuuskopiota

Kuten kuvio 6 nähdään, varmuuskopion puuttumista pidettiin toiseksi suurimpana uhkana yrityksessä. Varmuuskopio, voisi puuttua esimerkiksi tilanteessa, jossa varmuuskopion tekeminen epäonnistuu automaattiselta järjestelmältä, eikä tätä

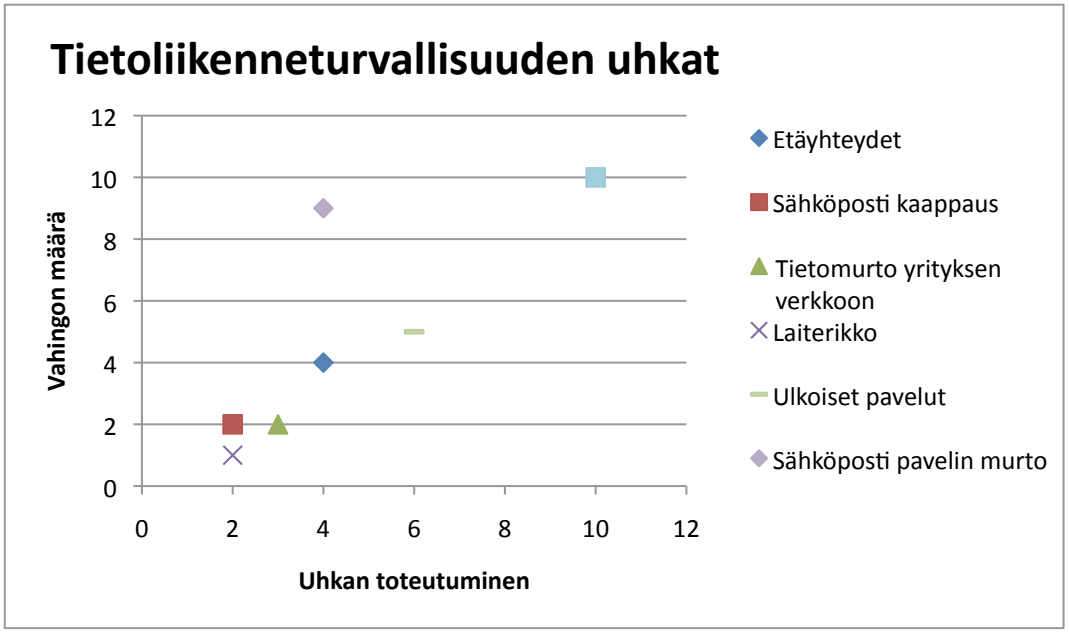
huomata ajoissa. Esimerkiksi yrityksen palvelin on asetettu varmuuskopioitumaan ulkoiselle tallennusmedialle. Mutta, jos tuntemattomasta syystä järjestelmä ei tee-kään varmuuskopiota. Jos tätä ei huomattaisi ajoissa, niin palvelimen kiintolevyn rikkoutuessa voisi hävitä oleellista dataa yrityksen toiminnan kannalta. (Miettinen, 1999, 239)

Yrityksen olisi hyvä tehdä pitkäaikainen varmuuskopio. Esimerkiksi kerran viikossa tai kuukaudessa (tämän tulisi olla säännöllistä) erillisen lisä varmuuskopion tekeminen ulkoiselle levylle ja varmuuskopion vieminen pois yrityksen tiloista, estäisi täydellisen katastrofin syntymisen. Jos normaali varmuuskopio pettäisi, voitaisiin silti palata, edes johonkin aikaisempaan tilanteeseen. Näin yritys parantaisi tietoturvaansa kaikkein tärkeimmän asian tiedon suojelemisessa. (Miettinen, 1999, 239.)

5.4.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella pyritään suojaamaan yrityksen verkossa liikkuva tieto, sekä kaikki tietoliikenne pyritään salaamaan, niin että sitä ei voida kuunnella. Laitetasolla tämä tarkoittaa palomuurien, reitittimien ja kytkimien asetusten asettamista oikein. Edellä mainituilla laitteilla, voidaan luoda fyysisesti tai virtuaalisesti eri verkkoja, sekä rajata tietoliikennettä. Jos yritys käyttää langattomia tekniikoita on tietoliikenneturvallisuudesta vastaavan hyvä tietää siitä aiheutuvat riskitekijät. Kuten jo murrettujen salaustekniikoiden käyttö kasvattaa tietomurron todennäköisyyttä. (Krutz & Vines, 2003, 110-111.)

Kuvio 7. Havainnollistaa, miten yritys on arvioinut tietoliikenne turvallisuuden riskejä. Kuvan horisontaalijana kertoo uhkan toteutumisen todennäköisyyden asteikolla 0-10. 0 = pienin mahdollinen todennäköisyys, 10 = suurin mahdollinen todennäköisyys. Vertikaalijana kertoo uhkan toteuttaman vahingon määrän. 0 = pienin mahdollinen vahinko, 10 = suurin mahdollinen vahinko.



Kuvio 7. Tietoliikenneturvallisuuden uhkat kohdeyrityksessä.

Etäyhteydet

Yritys käyttää etäyhteyksiä palvelimilleen VPN-tunneloinnin kautta. Yrityksessä kuitenkin koettiin, että etäyhteyden käyttäminen tietomurtoon, olisi jokseenkin epätodennäköistä. Kuten kuva 7 osoittaa, etäyhteyksistä aiheutuva haitta on myös suhteellisen pieni. Yritys pyrkii suojaamaan etäyhteyksiä, myös palvelimissa olevilla lokitiedoilla, jotta voidaan jälkeenpäin määrittää, kuka on tehnyt ja mitä. (CISCO) Etäyhteyksien osalta yritys ei oikeastaan voi enää parantaa tietoturvallisuuttaan.

Sähköpostin kaappaus

Lähtevien sähköpostien kaappaus on käytännössä mahdollinen, koska yritys ei käytä SSL-salausta sähköpostipalvelimessaan. Kaappauksen todennäköisyys arvioitiin kuitenkin suhteellisen pieneksi. Kuten kuviosta 7 voidaan todeta yksittäisen sähköpostin kaappauksesta aiheutuva haitta on hyvin pieni.

Yritys voisi helposti parantaa tietoturvaansa merkittävästi mm. asettamalla SSL-salauksen päälle, jolloin sähköpostien kaappaaminen olisi huomattavasti hankalampaa, eikä varmasti olisi vaivan arvoista. (Symantec)

Tietomurto yrityksen verkkoon

Tietomurron tekemistä yrityksen verkkoon pidettiin epätodennäköisenä. Pelkkä verkoon pääseminen ei aiheuta yritykselle merkittävää haittaa. Kuvio 7 osoittaa, yritys pitää huolta verkoistaan ja niiden salauksesta. Huolimatta siitä että yritys käyttää langattomia verkkoja on niiden salaus tapa vahva. Kuten yllä jo mainittiin ei pelkkä verkkoon pääseminen aiheuta yritykselle merkittävää haittaa. Tunkeutujan on haittaa aiheuttaakseen, myös saatava tietoonsa tunnuksia ja salasanoja yrityksen eri palveluihin. Yrityksen ei ole viisasta tehostaa tietoturvaansa, esimerkiksi poistamalla langattomia verkkoja. Koska tämä haittaisi yrityksen toimintaa ja hidastaisi oleellisesti päivittäisiä toimia. Yritys katsoo langattomista verkoista tulevan hyödyn suurempana, kuin haitan ja näin ollen hyväksyy niistä aiheutuvan riskin.

Laiterikko

Yrityksen verkko koostu useista reitittimistä, kytkimistä, virtuaaliverkoista, sekä palvelimista. Kuten kuvio 7 osoittaa, yritys ei kokenut laiterikon aiheuttamaa uhkaa tai haittaa suurena, koska laitteet olivat nopeasti korvattavissa, sekä yrityksellä on useita verkkoja, joita voidaan tarvittaessa käyttää. Palvelimista yritys pitää varmuuskopiota, jotka voidaan palauttaa tarvittaessa uudelle palvelimelle hyvinkin nopeasti.

Ulkoiset palvelut

Ulkoisilla palveluilla tarkoitetaan yrityksen käyttämiä palveluita, joita se ei itse tuota. Yritys käyttää mm. Tiedoston tallennus palveluita, josta tieto on saatavissa kuten verkkolevyltä. Kuten kuvio 7 käy ilmi, uhkan toteutumista voidaan pitää mahdollisena, sekä siitä aiheutuvaa haittaa merkittävänä. Vaikka ulkoisiin palveluihin ei viedä yrityksen arkaluontoisimpia materiaaleja on palveluissa olevan materiaalin määrä suuri. Kuitenkin tiedot on hajautettu useaan eri palveluun, joten kaikkien tietojen saaminen on epätodennäköistä.

Yrityksen olisi viisasta harkita tietojen siirtämistä omalle palvelimelle. Luomalla oma vastaavanlainen palvelu yrityksen sisäiseen käyttöön, yritys ei olisi riippuvainen ulkoisen palvelutarjoajan tietosuojasta tai sen heikkouksista.

Sähköposti palvelinmurto

Kuten kuvio 7 nähdään, yritys ei pitänyt uhkaa sähköpostipalvelin murrosta suurena. Toisaalta haitta, jonka se aiheuttaisi, olisi merkittävä. Murtautujalla olisi mahdollisuus saada haltuunsa, koko yrityksen sähköposti historia. Yritys käyttää kaikki mahdollisia suojaus keinoja, tämän estämiseksi.

6 PÄÄTELMÄT

Tutkimukseni tarkoituksena oli selvittää tietoturva kartoituksen kautta, mikä on yrityksen tietoturvan nykytila. Näin yrityksen johto saisi selkeämmän kuvan tietoturvan nykytilasta yrityksessä. Kartoitus antaa myös yrityksen johdolle suuntaa, mitä parannettavaa sen tietoturvassa on. Ensin oli kuitenkin selvitettävä miten tehdä tietoturva kartoitus. Kirjallisuudesta, sekä internetistä löytyi lähinnä ohjeita isoille yrityksille. Koin, että tarvittavan teoriatiedon hankkiminen oli haastavaa, joskin ei mahdotonta. Siksi päädyin muokkaamaan lähteistä saamani tiedon soveltuvaksi kohdeyritykselle. Osa tietoturvaan liittyvistä asioista, oli kehittynyt projektin myötä minulle itsestäänselvyydeksi. Koin ne hyvin vaikeaksi selittää, koska lähteitä niiden perusteluun oli haastava etsiä.

Projektin rajaaminen tuotti monesti ongelmia, koska tietoturva on hyvin laaja käsite. Projektia jouduttiin kuitenkin rajaamaan hyvinkin rajusti, lähinnä avainkohtiin osa-aluetta kohden. Siksi tuntui, että työstä olisi tullut osittain hyvin suppea ja yleispätevä. On kuitenkin muistettava, että tietoturvakartoituksen tarkoitus on antaa yritykselle näkemys sen tietoturvan nykytilasta, sekä osoittaa onko sen tietoturvassa parannettavaa.

Koen, että onnistuin antamaan yritykselle arvokasta tietoa siitä, mikä on yrityksen tietoturvan tämän hetkinen taso, sekä mitä parannettavaa yrityksellä on tietoturvan osalta. Yritys sai myös arvokkaita työkaluja, joilla se voi arvioida tietoturvaansa, sekä jatkuvasti muuttuvia uhkia. Jatkoa ajatellen yrityksen olisi hyvä tehdä kokonainen tietoturvasuunnitelma, joka pohjautuu tähän tietoturvakartoitukseen. Osa henkilökunnasta halusi lisää tietoa yrityksen tietoturvapolitiikasta ja toimintatavoista. Tietoturvapolitiikka ja toimintatavat olisi siis hyvä käydä läpi yrityksen henkilöstön kanssa.

Tämä tutkimus antoi yritykselle, myös parannus ehdotuksia jo ennestään hyvällä tasolla olevaan tietoturvaan. Yritys voisi kuitenkin helposti parantaa joitakin asioita pienellä vaivalla, kuten esimerkiksi seuraavilla toimilla, kuukausittaisen varmuuskopion tekeminen palvelimesta, joka sijaitsisi eri tiloissa, kuin yritys. Myös sähköpostin SSL-salaus olisi helppo tapa nostaa merkittävästi yrityksen tietotur-

vaa. Yksi laitteiston tietoturvaa merkittävästi nostava tekijä olisi find my device-palvelun aktivointi kaikkiin yrityksen mobiili laitteisiin. Näin laitteet olisivat jäljitettävissä.

Uskon kuitenkin itse saaneeni eniten hyötyä koko projektista. Projektin aikana sain lisää uutta tietoa tietoturvasta, sekä tietoturvan kartoittamisesta. Huomasin myös nopeasti, että tietoturva-asiat eivät ole niin helppoja, kuin voisi olettaa. Monelle voi tulla yllätyksenä, ettei kyse ole ainoastaan viruksista, sekä tietoliikenteestä, joita voi suojata virustorjunnalla ja palomuurilla. Ainoastaan 20% tietoturvasta on tietotekniikkaa, loput 80% on puhtaasti fyysistä tietoturvaa.

7 TIETOTURVAN TULEVAISUUS

Vaikka yrityksen tietoturva kohdeyrityksessä voidaan sanoa olevan hyvällä tasolla. On mediassa useita esimerkkejä, huonon tietoturvatason omaavista yrityksistä. Kuten ESS artikkelissaan verkkosivuilla toteaa ”Hölmöily tietoturvan kanssa saattaa lähitulevaisuudessa käydä kalliiksi. Euroopan komissio ehdottaa tietosuojaviranomaisille sakotusoikeutta.” Artikkelissa todetaan myös, ettei läheskään kaikki yritykset huolehdi asiakkaidensa henkilötiedoista lain velvoittamalla tavalla. Artikkelin mukaan, osa tarkastukseen joutuneista yrityksistä totesi, etteivät he tiedä, millä tavoin laki heitä velvoittaa suojaamaan asiakkaiden henkilötietoja. (Etelä-Suomen Sanomien verkkosivu, 22.10.2012)

Voidaan siis todeta, että tulevaisuus näyttää synkältä. Tasapainotellessa ohuella nuoralla, jossa putoamiasen uhkana on joutua tietoturva varkauden uhriksi. Sekä saada sakkoja tietoturvan laiminlyömisestä. Tulevaisuudessa yritysten on siis entistä tärkeämpää huolehtia tietoturvastaan. Tietoturvaa voidaan pitää jatkuvasti kehittyvänä osana yrityksen liiketoimintaa. Tulevaisuus näyttää, pystyvätkö yritykset suojaamaan tietonsa rikollisia vastaan, vai saavatko rikolliset yliotteen. Tässä jatkuvassa suojausten ja murtojen kilpajuoksussa.

LÄHTEET

Apple iCloud [viitattu: 25.10.2012] Saatavissa: http://www.apple.com/fi/icloud/

Apple OSX Mountain Lion [viitattu:25.10.2012] Saatavissa: http://www.apple.com/fi/osx/whats-new/

Baskerville, R.; Goodman, S; Straub, D. 2008. Information Security. Policy, Processes and Practices. M.E. Shape Inc.

Caelli, W; McCullagh, A. 2000. Non-Repudation in the digital Enviroment [viitattu 25.10.2012] Saatavissa: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/778/687

CISCO 2012, How virtual private networks work [viitattu 25.10.12] Saatavissa: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.shtml

Etelä-Suomen Sanoamat verkkosivu artikkeli, tietosuojavaltuutetulle kaavaillaan sakotusoikeutta [viitattu 25.10.2012] Saatavissa: http://www.ess.fi/?article=389296

Georgy, P. 2008. IT Disaster Recovery Planning For Dummies. John Wiley & Sons.

Hakala, M. Vainio & Vuorinen, O. 2006 Tietoturvallisuuden käsikirja. Jyväskylä: Docendo

Harju, E. 2010. Tietoturvasta huolehtiminen on elinehto. Varsinais-Suomen Yrittäjä 3/2010, 23

Hirsjärvi, S.,Remes, O. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. Uudistettu painos. Helsinki: Tammi.

ISO (International Organization for Standardization). ISO/IEC 17799 2000.

ISO (International Organization for Standardization). ISO/IEC 27001 2005.

ISO/IEC 17799 2000, [viitattu 25.10.2012] Saatavissa: http://www.iso.staratel.com/ISO17799/Doc/ISO17799/iso1799.pdf

ISO/IEC 27001 2005, [viitattu 25.10.2012] Saatavissa: http://www.cert.sd/images/stories/iso27001.pdf

Kurtz, R. L. & Vines R. D. 2003. Tietoturvasertifikaatti. CISSP. Suom. Suominen, E. Helsinki Edita Publishing Oy.

Laaksonen, M.; Nevasalo, T. & Tomula K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja laisäädäntö. Helsinki: Edita Publishing Oy.

Maiwald, E.; Sieglein, W. 2002. Security Planning and Disaster Recovery. McGraw-Hill Professional

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen. Näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media Oy.

Pentti Routio 1. Toteava havainnointi ja koe[viitattu 25.10.2012] Saatavissa: http://www2.uiah.fi/projects/metodi/062.htm - systhav

Pentti Routio 2. Kyselevät tutkimustavat [viitattu 25.10.2012] Saatavissa: http://www2.uiah.fi/projekti/metodi/064.htm - kysely

Raggard, B. G. 2010. Information Security Management. Concepts and Practice. Boca Raton: CRC Press.

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo Finland Oy.

Suvi Vuorela, Haastattelumenetelmät, 39-40 [viitattu 25.10.2012] Saatavissa: http://www.cs.uta.fi/usabsem/luvut/3-Vuorela.pdf

Symantec. Secure Sockets Layer (SSL): How it works [viitattu 25.10.2012] Saatavissa: http://www.symantec.com/theme.jsp?themeid=how-ssl-works

Taloustutkimusalitos verkkosivu 2012. [viitattu 25.10.2012] Saatavissa: http://www.taloustutkimus.fi/tuotteet_ja_palvelut/tiedonkeruuratkaisut_ja_monitila/kvalitatiivinen_tutkimus/

Tietoturvaopas. 2010. [viitattu 25.10.2012] Saatavissa: http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/

Tilastokeskuksen verkkosivu. [viitattu 25.10.2012] Saatavissa: http://www.stat.fi/virsta/tkeruu/04/03/

Viestintäviraston verkkosivu [viitattu 16.08.2012] Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

Virtuaali AMK verkkosivua 2012 http://www.amk.fi/opintojaksot/0709019/1193463890749/1193463919223/1193464257338/1193665318635.html

VTT. 2009. [viitattu 25.10.12] Saatavissa: http://virtual.vtt.fi/virtual/riskianalyysit/index273b.html

LIITTEET

Liite 1. ESS-lehtiartikkeli 22.10.2012

KOTIMAA

Tietosuojavaltuutetulle kaavaillaan sakotusoikeutta

22.10.2012 3:00

Tietosuojavaltuutettu Reijo Aarnion mielestä sakotusoikeus olisi hyvä lisä tietoturvaviranomaisen keinovalikoimaan. Kuva: Lehtikuva

Hölmöily tietoturvan kanssa saattaa lähitulevaisuudessa käydä kalliiksi. Euroopan komissio ehdottaa tietosuojaviranomaisille sakotusoikeutta.

Seuraamusmaksu liikeyrityksille olisi lainrikkomuksesta riippuen jopa kaksi prosenttia liikevaihdosta. Muiden kuin yritysten, kuten oppilaitosten, sakko olisi korkeintaan miljoona euroa.

Kyse on todellisesta pelotteesta. Miljardiyritystä sakko voisi kirpaista kymmenillä miljoonilla euroilla.

Ajatus sakotusoikeudesta sisältyy EU:n ehdotukseen uudesta tietosuoja-asetuksesta. Komission tavoitteena on saada päätös sakotusoikeudesta ennen vuotta 2014. Siirtymäaika olisi kaksi vuotta, mutta esimerkiksi sakotusoikeus voisi tulla voimaan tätä nopeammin.

Suomen tietosuojavaltuutetun Reijo Aarnion mielestä sakotusoikeus olisi hyvä lisä tietoturvaviranomaisen keinovalikoimaan. Hän muistuttaa, ettei uudistuksen tarkoitus ole luoda valtiolle raha-automaattia vaan oikeasti parantaa tietosuojaa.
-Idea ei kuitenkaan ole lyödä kovaa vaan se, että yritykset ottaisivat opikseen.

Läheskään kaikki suomalaisyritykset eivät huolehdi henkilötiedoista niin kuin pitäisi.

Tietosuojavaltuutettu teki kesällä tarkastuksen 74 yritykseen tai yhteisöön, joiden tietoturvaa loukattiin laajassa tietomurtojen aallossa loka-joulukuussa 2011. Joka kolmas ei ollut tehnyt tietosuojaansa mitään muutoksia

Kymmenet tunnustivat, etteivät tiedä, millä tavoin laki velvoittaa heitä suojaamaan asiakkaiden henkilötiedot.

STT

Liite 2. Tietoturvakysely kohdeyrityksen työntekijöille.

Tämän kyselyn tarkoituksena on kartoittaa Yritys-X henkilökunnan tietoturva-osaamisen tasoa. Kysymykset mittaavat perus tietoturva tietämystä yrityksen arjessa. Kysely tullaan esittämään kaikille yrityksessä työskenteleville henkilöille. Kysely toteutetaan kirjallisena.

Ohjeistuksena vastaajille: Tämä kysely ei ole kilpailu, eikä koe. Tarkoituksena ei ole saada mahdollisimman paljon oikeita vastauksia, vaan kartoittaa, mikä on työntekijöiden tietämys tietoturvasta tällä hetkellä. Siksi toivon, että kukaan vastaajista ei käytä tietolähteitä vastatakseen kysymyksiin, vaan vastaa rehellisesti käyttäen ainoastaan omaa tietämystään. Näin saadaan mahdollisimman realistinen kuva työntekijöiden tietoturva tietämyksestä tällä hetkellä.

1 . Kerro millainen on vahva salasana?

2. Onko seuraava väittämä totta? Jotta muistaisin salasanani voin käyttää samaa salasanaa kaikissa kohteissa. Perustele vastauksesi.

3. Miten toimit työssäsi tulosteiden kanssa, joita ei tarvita, niiden sisältäessä esimerkiksi asiakas tietoja?

4. Onko seuraava väittämä totta? Kun alustat muistitikun tietoja ei voida enää palauttaa. Perustele vastauksesi.

5. Onko seuraava väittämä totta? Kun haluat poistaa tiedoston koneelta, heität tiedoston roskakoriin ja tyhjennät roskakorin. Tiedostoa ei voida enää palauttaa roskakorin tyhjennyksen jälkeen. Perustele vastauksesi.

6. Onko seuraava väittämä totta? Kun näytät asiakkaalle tietoja koneen näytöltä on varottava, ettei hän näe muita hänelle kuulumattomia tietoja. Perustele vastauksesi.

7. Yrityksen tiloihin tulee henkilö ja kertoo olevansa hälytin laitteiden korjaaja. Miten varmistut, että henkilö on se kuka hän sanoo olevansa?

8. Pidätkö tietoturvaa tärkeänä asiana? Perustele vastauksesi.

9. Haluaisitko saada enemmän tietoa ja ohjeistusta tietoturvasta, sekä yrityksen tietoturva politiikasta?